Escuela de Negocios
Tipo de documento: Tesis de maestría

Master in Management + Analytics

Los problemas sin retorno que una caída de Lido podría traer a las finanzas descentralizadas

Autoría: Rodríguez Pisani, Matías Demián
Año: 2025

UNIVERSIDAD TORCUATO DI TELLA

Master in Management + Analytics

Los problemas sin retorno que una caída de Lido podría traer a las finanzas descentralizadas

Alumno: Matias Demián Rodriguez Pisani

Tutor: Lionel Modi

Contenidos

Resumen

La implementación de Lido cambió el problema de liquidez que depositar tokens en la blockchain conlleva, incluyendo operaciones con los protocolos de finanzas descentralizadas más grandes.

El objetivo de este trabajo es medir y analizar los riesgos que errores en Lido podrían generar para el ecosistema, pudiendo cuantificar los mismos y proponer algunas soluciones. Además, se explicará el funcionamiento de Lido, y las ventajas que brinda.

El conjunto de datos incluirá una mezcla de las métricas más importantes, como puede ser el total depositado en protocolos, en cuáles protocolos, su composición y su evolución. Como así también se proporcionará información sobre las penalizaciones a los validadores de ethereum.

El modelo creado analiza y mide el máximo de pérdida que puede afrontar Lido en un caso extremo, buscando de esta forma concientizar sobre los distintos escenarios que podrían afrontarse ante fallas en los validadores.

Revisión de Literatura

El estudio de blockchain y las finanzas descentralizadas (DeFi) ha sido abordado desde múltiples enfoques en la literatura académica y técnica. Investigadores han explorado tanto los aspectos fundamentales de la tecnología blockchain, como sus aplicaciones en el ámbito financiero, y los riesgos asociados a nuevas formas de participación, como el staking líquido. Esta revisión analiza investigaciones clave que han aportado al entendimiento de estas áreas y proporciona una base para evaluar la solución de staking líquido que ofrece Lido en Ethereum.

Estudios sobre Blockchain y Descentralización

La descentralización es un tema central en la investigación sobre blockchain. Buterin (2017) introduce el concepto de descentralización en tres dimensiones: arquitectónica, política y lógica. Estos aspectos son fundamentales para entender cómo las blockchains como Ethereum se diferencian de los sistemas centralizados tradicionales. Otros estudios, como los de Schär (2019), profundizan en cómo la descentralización de blockchain ofrece ventajas como la resistencia a la censura y la eliminación de intermediarios, elementos que son críticos en el desarrollo de aplicaciones financieras descentralizadas.

Por otro lado, investigaciones como las de Warwick (2020) señalan que la descentralización también introduce desafíos técnicos y de gobernanza. Estos estudios proporcionan un marco teórico para evaluar las diferentes implementaciones de blockchain y sus mecanismos de consenso, que son esenciales para asegurar la integridad y seguridad de las redes descentralizadas.

Finanzas Descentralizadas (DeFi)

En el ámbito de las finanzas descentralizadas, autores como Schär (2021) han analizado cómo las finanzas descentralizadas permiten la creación de mercados financieros abiertos y sin permisos a través del uso de contratos inteligentes. La literatura destaca que DeFi ha transformado el acceso a servicios financieros, eliminando intermediarios tradicionales, como bancos, y permitiendo transacciones persona a persona más eficientes.

Estudios como los de Lutsenko (2021) y Breitner et al. (2022) señalan que, aunque el crecimiento de DeFi ha sido exponencial, existen riesgos inherentes relacionados con la seguridad de los contratos inteligentes y la falta de regulaciones. La investigación de Hussain et al. (2022) también identifica el problema de la interoperabilidad entre diferentes plataformas y los riesgos asociados a la interconexión de protocolos, un tema particularmente relevante para entender el impacto de Lido en el ecosistema DeFi.

Staking líquido y Lido

El staking líquido, introducido principalmente por protocolos como Lido, ha sido objeto de estudio por su capacidad para resolver uno de los principales problemas del staking tradicional: la falta de liquidez. Estudios recientes han examinado cómo Lido permite a los usuarios mantener la liquidez de sus activos en staking a través de la emisión de tokens derivados como stETH y wstETH (Lido Blog, 2023).

Riesgos de slashing y modelos de cobertura

El fenómeno del slashing ha sido ampliamente discutido en estudios que evalúan los riesgos del modelo Proof of Stake (PoS). Buterin (2017) y Edgington (2023) destacan cómo el slashing actúa como un mecanismo para garantizar la honestidad de los validadores, pero al mismo tiempo introduce el riesgo de que los validadores pierdan una parte significativa de sus fondos en staking. Este riesgo es particularmente elevado para protocolos como Lido, que dependen de la operación eficiente de múltiples operadores de nodos.

Lido Finance (2022) ha realizado simulaciones y análisis de riesgo para evaluar cómo el protocolo enfrentaría un evento de slashing masivo. Estos estudios son importantes porque demuestran que, aunque Lido ha implementado un fondo de cobertura para mitigar estos riesgos, en escenarios extremos podría no ser suficiente para cubrir todas las pérdidas. En estos casos, la pérdida de confianza en el protocolo podría generar una crisis de liquidez, con efectos adversos tanto para Lido como para el ecosistema DeFi en general.

1. Introducción

Las finanzas descentralizadas (DeFi) nacieron como una innovación en la intersección del mundo financiero y la tecnología blockchain, ofreciendo una infraestructura financiera que es abierta, interoperable y transparente. A través del uso de contratos inteligentes, DeFi ha logrado replicar servicios financieros tradicionales de manera más accesible y sin la necesidad de intermediarios centralizados, como los bancos (Schär, 2019).

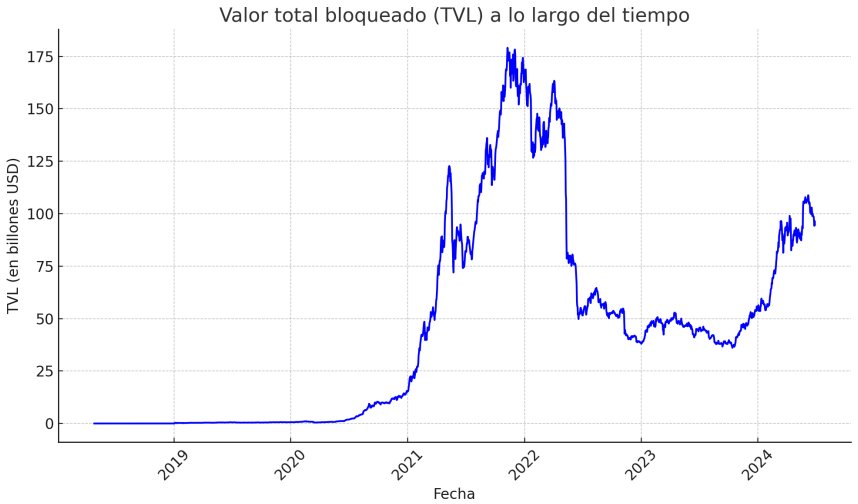


Figura 1. Fuente: https://defillama.com/

La adopción de aplicaciones y protocolos de finanzas descentralizadas ha sido uno de los fenómenos más notables en el espacio blockchain en los últimos años. Según datos de DeFiLlama, el valor total depositado en los contratos inteligentes, sin segmentar por ninguna blockchain, era de USD 675.000 en enero de 2019. A partir de ese momento, su crecimiento fue exponencial, llegando a un pico de USD 178.000 millones en noviembre de 2021. Actualmente, se encuentra en aproximadamente USD 50.000 millones.

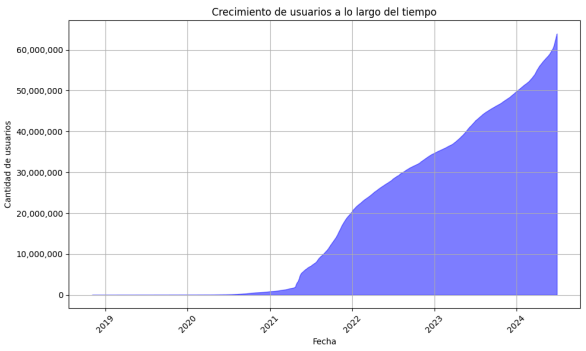


Figura 2. Fuente: https://dune.com/rchen8/defi-users-over-time

El número de usuarios únicos de los protocolos DeFi creció exponencialmente, pasando de unos pocos miles a millones desde 2021. Esta explosión en las cifras no es casualidad, el objetivo de las finanzas descentralizadas es democratizar el acceso a servicios financieros, eliminando intermediarios y permitiendo transacciones seguras y transparentes (Schär, 2019). A diferencia de las finanzas tradicionales, donde los intermediarios y las instituciones centralizadas juegan un papel crucial, DeFi se basa en protocolos abiertos y aplicaciones descentralizadas (DApps) que funcionan sobre plataformas de contratos inteligentes, como Ethereum, en este caso, la seguridad es a la vez el punto más importante, y más frágil a la vez. Estos contratos inteligentes, que son programas almacenados en la blockchain y ejecutados de manera simultánea por una red de validadores, aseguran un alto nivel de seguridad y transparencia en cada operación (Schär, 2019).

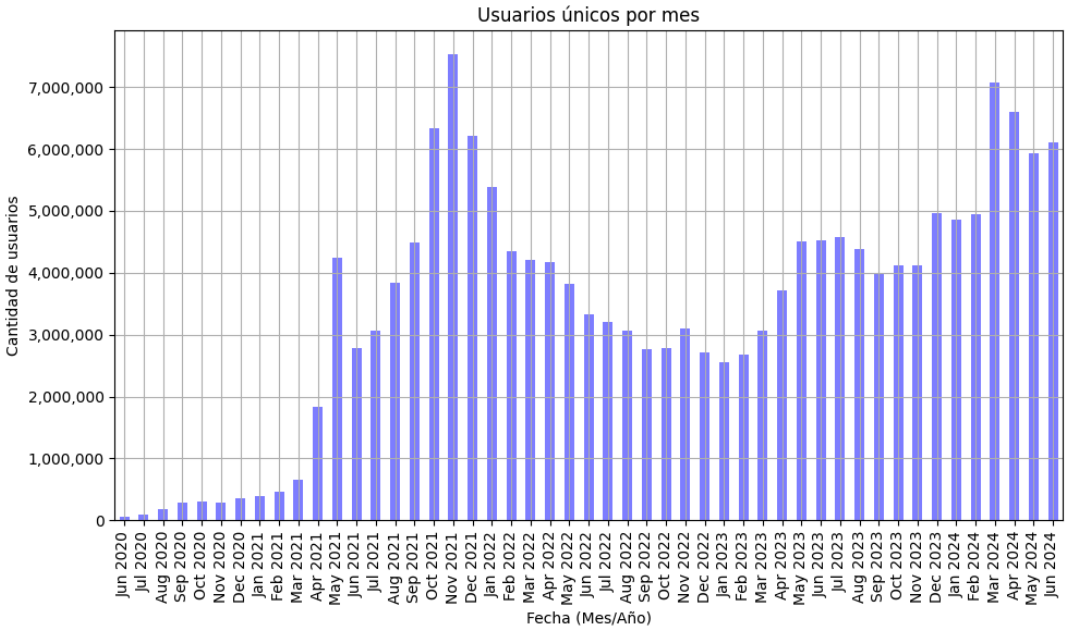


Figura 3. Fuente: https://dune.com/rchen8/defi-users-over-time

No es un detalle menor la intención de dejar atrás la clásica y tradicional figura de los bancos. Sin embargo, el continuo avance y consolidación del espacio DeFi depende de una infraestructura robusta y segura, lo cuál también posee sus limitaciones. En el caso de Ethereum, esto se basa en gran medida en el mecanismo de consenso de la red.

Aunque el staking, definido como el proceso en el cual los usuarios bloquean sus activos en una red blockchain para apoyar las operaciones de la red, como la validación de transacciones y la seguridad, abrió puertas a oportunidades de inversión sin antecedentes, también generó un dilema: el equilibrio entre participación activa vs. pérdida de liquidez. Tradicionalmente, staking en Ethereum significaba inmovilizar activos para darle seguridad a la red, una barrera que muchos inversores no estaban dispuestos a cruzar. Acá es donde el staking líquido llegó para modificar la forma de realizarlo. Esta

modalidad permite a los usuarios disfrutar de los beneficios del staking mientras retienen la capacidad de mover y comerciar sus activos con facilidad.

Lido, el principal protocolo que habilita esta operatoria, no es simplemente otro actor en el espacio de finanzas descentralizadas; es una de las soluciones pioneras que busca resolver este dilema de liquidez. Ethereum, con su transición a la Prueba de Participación (PoS, por sus siglas en inglés), inaugura una nueva era en la forma en que se validan y se garantizan las transacciones. Este mecanismo de consenso selecciona a los validadores en función de la cantidad de criptomonedas que poseen y están dispuestos a bloquear como garantía, reemplazando al sistema anterior basado en la Prueba de Trabajo (PoW). A diferencia de PoW, donde el proceso de minería consumía enormes cantidades de energía, PoS introduce un enfoque más eficiente y sostenible, en el que los validadores bloquean una suma de su ETH como garantía para participar en el proceso de validación.

Esta nueva arquitectura, viene con nuevos desafíos. Uno de los mayores es la noción de "slashing". En PoS, sí un validador se comporta de manera contraria a las reglas del protocolo, ya sea por error o por algún incentivo malicioso, una fracción o incluso la totalidad de sus fondos bloqueados puede ser confiscada. Esta penalización busca desincentivar cualquier comportamiento inapropiado y garantizar la seguridad de la red, pero también impone un riesgo significativo para aquellos que bloquean grandes sumas de ETH en staking.

Hay tres maneras en que un validador puede ser objeto de sufrir este fenómeno, todas las cuales se reducen a la propuesta o atestiguamiento deshonesto de bloques:

- Proponer y firmar dos bloques diferentes para el mismo espacio de tiempo.
- Atestiguar un bloque que "rodea" a otro (efectivamente cambiando la historia).
- "Votación doble" atestiguando dos candidatos para el mismo bloque.

Si estas acciones son detectadas, el validador es objeto de slashing. Esto significa que 1/32 de su ether apostado se quema inmediatamente, y luego comienza un período de eliminación de 36 días. Durante este período, el depósito del validador se va reduciendo gradualmente, donde 18 días es el punto medio, y en ese momento, se aplica una penalización adicional cuya magnitud escala con el ETH total apostado de todos los validadores slasheados en los 36 días anteriores al evento.

Esto significa que cuando más validadores son objeto de slashing, mayor es la magnitud de la penalización. El máximo slashing es el balance efectivo total de todos los validadores slasheados. Por otro lado, un evento de slashing aislado y único solo quema una pequeña porción del bloqueo del validador. Esta penalización intermedia que escala con el número de validadores slasheados se llama "penalización por correlación".

Lido, como protocolo que permite el staking líquido, enfrenta desafíos adicionales en este entorno. Su estructura depende de múltiples operadores de nodos para gestionar y operar los validadores en nombre de sus usuarios. Si bien esta diversificación puede ofrecer cierta protección contra fallos individuales, también presenta el riesgo de que problemas con uno o más operadores puedan afectar de manera desproporcionada al ecosistema.

Además, el diseño del protocolo introduce el stETH, un token que busca representar el valor del ETH en staking, pero con la característica de ser líquido. Cualquier impacto en la paridad entre stETH y ETH podría afectar la confianza en el protocolo, llevando potencialmente a fluctuaciones de precio o, en el peor de los casos, a retiros masivos que lo desestabilicen.

Finalmente, vale la pena mencionar la interacción de estos riesgos con el ecosistema más amplio de DeFi. La relación entre stETH y otras plataformas, préstamos, y derivados es cada vez mayor. Un impacto en Lido podría tener efectos en cadena en otros protocolos, y viceversa.

El objetivo principal de este trabajo es, por lo tanto, entender las complejidades y los desafíos que subyacen en el corazón de Lido y su modelo de staking líquido, con un enfoque particular en los riesgos que podrían emerger si sus validadores enfrentan problemas. Comprender estos riesgos no es solo una cuestión académica; representa una necesidad crítica para los participantes del mercado, los reguladores, y cualquiera que tenga interés en construir sobre la promesa de las finanzas descentralizadas.

Este proceso será iniciado con una inmersión en la naturaleza del staking líquido, innovación que permite a los usuarios participar en sistemas de consenso mientras siguen manteniendo liquidez sobre sus activos. Es crucial entender cómo Lido implementa esta propuesta, cuáles son los incentivos para los validadores, y qué mecanismos existen para garantizar que actúen en el mejor interés de la red. Este entendimiento proporcionará una base sobre la cual podremos identificar puntos de fallo potenciales y áreas de vulnerabilidad.

Todo esto permite entender y dimensionar un posible escenario catastrófico que podría tener sobre este mercado una pérdida del valor o peg del token de stETH demostrando así la interdependencia que caracteriza a las finanzas descentralizadas, donde la fortaleza o la debilidad de un único protocolo puede tener fuertes efectos de contagio sobre el resto. Aún peor, esto nos va a permitir también dimensionar el impacto que tendría sobre la red de Ethereum y su seguridad.

2. El origen de la blockchain

La génesis de la tecnología blockchain se encuentra profundamente arraigada en la confluencia de la crisis financiera de 2008 y el avance de la digitalización global. Este período de incertidumbre económica y desconfianza en las instituciones financieras tradicionales originó un terreno fértil para el desarrollo de sistemas alternativos de transacciones y registros.

En este contexto, la blockchain emergió como una solución innovadora, ofreciendo un nuevo paradigma para el manejo y registro de transacciones digitales. La idea central era crear un sistema que permitiera interacciones financieras directas entre las partes, eliminando la necesidad de intermediarios. Este concepto fue implementado por primera vez con éxito en la creación de Bitcoin, una moneda digital descentralizada. La blockchain, como su columna vertebral, fue presentada como un libro mayor distribuido, inmutable y transparente, que registraba todas sus transacciones.

La estructura de la blockchain se basa en una serie de bloques interconectados, cada uno conteniendo un grupo de transacciones. Una vez que un bloque se añade a la cadena, alterar su contenido se vuelve extremadamente difícil debido al requisito de modificar todos los bloques subsiguientes, lo que a su vez necesitaría un consenso de la mayoría de la red. Esta característica de inmutabilidad no solo asegura la integridad de los registros sino que también sirve como un mecanismo de seguridad robusto y contundente.

Más allá de Bitcoin, el potencial de la blockchain para revolucionar diversos aspectos de las transacciones y los registros digitales comenzó a ser reconocido. La tecnología ofrecía no solo una plataforma para transacciones financieras sino también para aplicaciones en diferentes sectores, desde la gestión de la identidad hasta los registros de propiedad, entre otros. Su capacidad para garantizar la seguridad, la transparencia y la resistencia a la manipulación la convirtió en una opción atractiva para una amplia gama de aplicaciones.

Es necesario nombrar además, un elemento fundamental que la blockchain posee, su naturaleza descentralizada. A diferencia de los sistemas centralizados, donde una entidad única ejerce y posee control total, la blockchain distribuye la gestión de su base de datos entre una red de nodos. Esto mejora la resistencia y la seguridad de la red, promoviendo así un sistema más democrático y resistente a la censura. Además, el uso de criptografía avanzada en la blockchain garantiza tanto la transparencia de las transacciones como la privacidad de los usuarios. Si bien todas las transacciones son públicamente auditables, la identidad de los usuarios permanece protegida, creando un equilibrio entre la transparencia y la privacidad.

Es así entonces como la blockchain surgió como una respuesta directa a las necesidades de un sistema financiero más transparente, seguro y eficiente, sentando las bases para una nueva era de interacciones digitales y abriendo el camino para una variedad de aplicaciones innovadoras.

3.Mecanismos de Consenso. Concepto y significado

Los mecanismos de consenso son fundamentales en el funcionamiento de las blockchains. Constituyen el método mediante el cual los participantes de esta red descentralizada acuerdan la validez de las transacciones y mantienen una versión coherente y unificada de este libro mayor. En un entorno sin una autoridad central, como previamente comenté, estos mecanismos aseguran que todas las partes involucradas tengan una visión consistente, precisa y única de la cadena de bloques.

Básicamente, el propósito principal de un mecanismo de consenso es resolver el problema de la confianza en un sistema descentralizado. En este mundo donde generalmente los participantes no se conocen ni necesariamente confían entre sí, es esencial tener un sistema que garantice que todas las transacciones y bloques sean legítimos y estén libres de manipulaciones. Este proceso no solo valida las transacciones sino que también previene el problema del doble gasto.

3.1 ¿Cuál es el problema del doble gasto?

Es un desafío digital crítico que surgió con la creación de las monedas digitales. Se refiere a la dificultad de asegurar que una unidad digital de valor solamente se puede gastar una y única vez, el surgimiento de esto es con los activos digitales porque, a diferencia del dinero físico, estos pueden duplicarse fácilmente. Si se le otorga un billete, quien lo tenía, ya no lo posee, dicho de otra forma, ya no podría dar el mismo billete a otra persona, esto evita el doble gasto de manera inherente gracias a la naturaleza física del dinero. Pero, en el mundo digital, sin llegar aún a la blockchain, no existía una forma sencilla y descentralizada de poder replicar esta propiedad física.

Este problema en los sistemas digitales tradicionales, como pueden ser por ejemplo los bancos o las tarjetas de crédito, se previene a través de un tercero de confianza que verifica y mantiene un registro de todas las transacciones. El problema de esta solución, es que es centralizada y depende de la confianza en estas instituciones.

3.2 Consenso

Un mecanismo de consenso eficaz debe lograr varios objetivos clave. Primero, debe garantizar la integridad y la inmutabilidad de la cadena de bloques, asegurando que una vez que un bloque se añade a la cadena, no pueda ser alterado retroactivamente sin el consenso de la red. Segundo, debe proporcionar

un método justo y transparente para que todos los nodos participen en el proceso de validación de transacciones y creación de bloques. Tercero, debe ser capaz de resistir ataques maliciosos, asegurando que ningún participante o grupo de participantes pueda tomar control de la red de manera fraudulenta.

En términos prácticos, un mecanismo de consenso actúa como el corazón de una red, bombeando regularmente nuevos bloques a la cadena y manteniendo el sistema vivo y funcionando correctamente. Es el mecanismo que permite que una red descentralizada opere de manera eficiente y segura, sin la necesidad de una autoridad centralizada que supervise y valide cada acción en la red.

Los mecanismos de consenso varían en complejidad y en el enfoque específico para lograr estos objetivos. Algunos se centran más en la seguridad, mientras que otros buscan maximizar la eficiencia o la equidad en la distribución de recompensas. La elección de un mecanismo de consenso adecuado es crucial para el diseño de cualquier blockchain, ya que define cómo se validan las transacciones, cómo se añaden nuevos bloques a la cadena y cómo se mantiene la integridad y la confiabilidad de toda la red.

3. 2 Tipos de mecanismos de consenso

3.2.1 Prueba de Trabajo (PoW)

El primero en entrar en escena fue el mecanismo de Prueba de Trabajo (PoW), un pionero que trajo la promesa de una red segura y descentralizada. Consiste en un ejército de mineros, donde cada uno tiene un poderoso poder de cómputo, y compiten en una carrera frenética para resolver acertijos matemáticos complejos. El ganador es el primero en descifrar el enigma, tiene en ese caso el honor de añadir un nuevo bloque a la cadena y, como recompensa, recibe una cantidad de la criptomoneda de la red, básicamente termina añadiendo un bloque a la cadena. Este proceso termina siendo robusto en seguridad, tiene un problema no menor, que es el gran consumo eléctrico que posee, y una gran barrera de entrada a quienes desean ser parte, que es poseer los recursos necesarios para obtener hardware de alta gama.

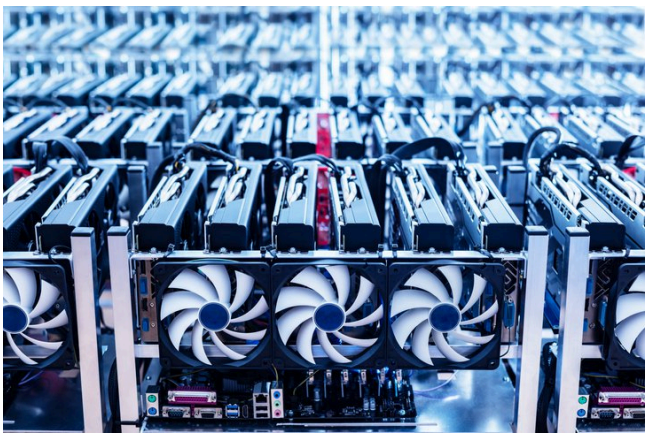


Figura 4. Granja de minería con placas de video.

3.2.2 Prueba de Depósito (PoS)

En busca de un equilibrio más sostenible y democrático, emerge el Proof of Stake (PoS). En este mundo, el poder no viene dado por la capacidad de resolver acertijos, sino por la confianza y la participación. En este mecanismo, los validadores son elegidos no por su potencia computacional, sino por la cantidad de monedas que poseen y, en ocasiones, por la lealtad demostrada a la red a través del tiempo. Este cambio representó una revolución, reduciendo drástica y fuertemente el consumo de energía, abriendo así las puertas a una mayor participación. No obstante, esta democratización lleva consigo preguntas sobre la distribución de poder, ya que aquellos con mayores tenencias tienen más influencia en la validación de transacciones.

3.2.3 Otros mecanismos

Más allá de estos dos gigantes, fueron emergiendo otros como puede ser la Prueba de Autoridad (Proof of Authority, PoA) o la Prueba de Participación Delegada (Delegated Proof of Stake, DPoS) que son ejemplos de cómo la comunidad blockchain sigue innovando. En PoA, los nodos validadores son preseleccionados, lo que acelera el proceso pero plantea interrogantes sobre la descentralización. DPoS, por su parte, ofrece un enfoque más democrático, donde los titulares de tokens votan por representantes para que realicen la validación en su nombre.

Cada uno de estos mecanismos plantea su propia historia de equilibrio entre seguridad, eficiencia energética, descentralización y equidad. La elección de uno sobre otro depende de las prioridades de cada red. Mientras que algunos buscan la fortaleza a través de la resistencia y la seguridad que ofrece PoW, otros prefieren la eficiencia y la participación inclusiva de PoS. En un mundo donde la tecnología

avanza a pasos agigantados, estos mecanismos de consenso evolucionan constantemente, buscando la fórmula perfecta para una red blockchain segura, eficiente y justa.

3. 3 Medición de la descentralización en blockchain

Este término se presta a múltiples interpretaciones, por lo que es necesario aclarar qué significa y cómo puede evaluarse, especialmente en el contexto de la seguridad, la resistencia a fallos y la distribución del control.

De acuerdo con Vitalik Buterin, la descentralización[1] puede analizarse en tres dimensiones clave:

- **Descentralización arquitectónica:** Hace referencia a la cantidad de nodos que componen una red y a la capacidad de la misma para resistir fallos de un número de ellos sin que se vea comprometida su operatividad.
- **Descentralización política:** Se refiere a cuántas personas o entidades tienen el control real sobre los nodos de la red y su capacidad de influir en las decisiones de gobernanza.
- **Descentralización lógica:** Implica la estructura de la red desde un punto de vista funcional. Si una red es lógicamente centralizada, se comporta como un sistema monolítico que no puede dividirse sin perder funcionalidad. En contraste, una red lógicamente descentralizada puede dividirse en múltiples partes, cada una capaz de operar de manera independiente.

La descentralización es esencial porque introduce resistencia a fallos, aumenta la dificultad de ataques maliciosos y previene la colusión entre actores que podrían comprometer la integridad del sistema. Estos aspectos permiten que las redes blockchain como Ethereum mantengan su seguridad y neutralidad sin depender de una autoridad central.

Para una medición más holística, también se pueden tener en cuenta otros factores, como la diversidad geográfica de los validadores y las implementaciones técnicas, ya que la concentración de validadores en una misma ubicación o el uso de software homogéneo también puede aumentar los riesgos de fallos comunes o ataques coordinados.

En conclusión, aunque los mecanismos de consenso son la base de la seguridad en una blockchain, la descentralización es lo que garantiza que esa seguridad sea robusta y resistente a fallos o ataques externos. A mayor descentralización arquitectónica, política y lógica, mayor será la capacidad de la red para mantener su integridad a largo plazo.

[1] Buterin, V. (2017, February 6). The Meaning of Decentralization. Medium. https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274.

4. ¿Qué es el staking en Ethereum?

El staking en Ethereum consiste en depositar 32 ETH para activar el software de validación. Como validador, se es responsable de almacenar datos, procesar transacciones y añadir nuevos bloques a la blockchain. Esta actividad no solo mantiene segura la red, y su eficiencia, sino que también permite ganar ETH adicional en el proceso.

Existen distintas formas de stakear ETH, la individual, como servicio, o la grupal. El staking individual consiste en tener al menos 32 ETH, y un equipo dedicado conectado a internet todo el tiempo. La segunda opción, como servicio, permite delegar la operación del nodo mientras continúas ganando recompensas. Un detalle no menor es que requiere un cierto nivel de confianza en quien provee el servicio ya que en ese caso, los ETH están siendo delegados. Por último, el staking agrupado o un pool de staking, es ideal para usuarios que no pueden ya que no poseen la totalidad necesaria o no se sienten cómodos stakeando 32 ETH.

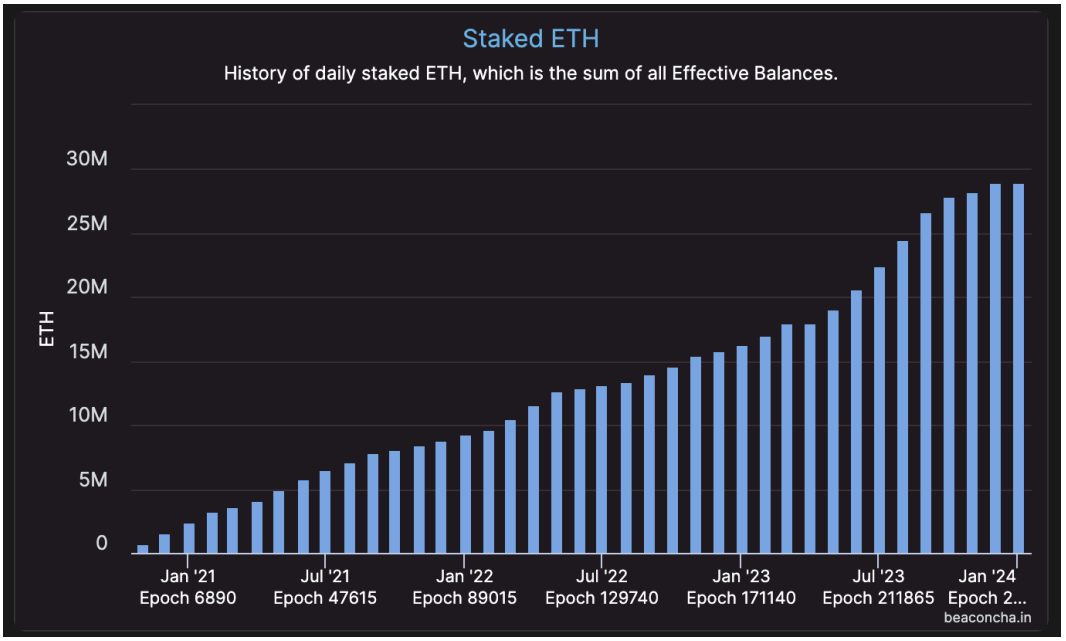


Figura 5. Fuente: https://beaconcha.in/charts

Cada una de estas formas posee sus riesgos. Para el caso del individual, existe la posibilidad de ser penalizado por desconexión del nodo, y además que sea “slasheado” por comportamiento malicioso. En el caso del staking como servicio, además de tener también los riesgos del individual, se agrega el riesgo asociado a delegarle la confianza de tus ETH al proveedor del servicio. Y por último, existe el agrupado,

que comparte los mismos riesgos que el individual con la diferencia de que el monto depositado es menor.

5. Lido: Solución para el staking líquido

Explicado todo lo anterior, resulta oportuno hablar sobre Lido, una innovación clave en el panorama de PoS. Lido emerge como una solución diseñada para maximizar la eficacia y accesibilidad en particular dentro del contexto de Ethereum 2.0.

Se posiciona en la vanguardia en búsqueda de abordar uno de sus desafíos más significativos: la liquidez. En un entorno PoS estándar, los participantes "stakean" sus criptomonedas como garantía para poder validar transacciones y, a cambio, reciben recompensas como ya fue explicado anteriormente. Sin embargo, este proceso tradicionalmente inmoviliza los activos de los participantes, limitando su liquidez y flexibilidad.

Lido revoluciona este enfoque con su propuesta de staking líquido donde permite a los usuarios participar en el proceso de “staking” sin renunciar a la liquidez de sus activos. Al depositar sus criptomonedas a través de Lido, los usuarios reciben tokens stETH (Lido Staked ETH) en proporción a su participación, donde también representan los intereses acumulados pero con la ventaja adicional de ser líquidos y comerciables. La gran ventaja es que este token stETH puede ser utilizado en otras actividades de DeFi, como préstamo, o como también garantía, permitiendo así al usuario continuar utilizando las finanzas descentralizadas sin ningún tipo de límite.

Lido se encarga de distribuir los ETH depositados entre varios validadores de la red, optimizando las posibilidades de ser seleccionados para validar bloques, y por ende, maximizar las recompensas potenciales para los usuarios. Esto convierte el “staking” en algo más flexible, y además contribuye a la descentralización y seguridad de la red.

stTokens: stETH y wstETH

Existen dos versiones de los stTokens de Lido: stETH y wstETH. Ambos son tokens fungibles, pero reflejan las recompensas acumuladas de forma distinta. stETH implementa una mecánica rebasable, lo que significa que el saldo de stETH aumenta de forma periódica, y por cada stETH existente hay un ether respaldándolo. Por otro lado, wstETH es un "constant token", cuyo valor eventualmente aumenta o disminuye si se compara con stETH. Dicho de otra forma, wstETH surge como una solución para facilitar las integraciones con el resto de protocolos de finanzas descentralizadas, y es el equivalente a stETH no rebasable que acumula valor.

En cualquier momento, cualquier cantidad de stETH puede convertirse en wstETH y viceversa. Un ejemplo de este proceso se da en el contexto de posiciones de wstETH con garantía insuficiente en MakerDao, las cuales pueden liquidarse convirtiendo el wstETH en ether a través de Curve u otros exchanges descentralizados.

En resumen, stETH es un token similar al estándar ERC-20, aunque no lo cumple estrictamente, ya que no emite un evento Transfer() en cada rebase. Un evento Transfer es una notificación en la blockchain que se emite cuando un token se mueve de una dirección a otra, lo que facilita el seguimiento de transferencias en los contratos inteligentes. Por su parte, un rebase es un mecanismo que ajusta automáticamente el balance de los tokens en las billeteras de los usuarios para reflejar cambios en el suministro total, como las recompensas de staking o las penalizaciones. stETH representa el ether depositado en el protocolo Lido, y a diferencia del ether, es líquido y puede ser transferido, comercializado o utilizado en aplicaciones de finanzas descentralizadas (DeFi). El suministro total de stETH refleja la cantidad de ether depositado en el protocolo, junto con las recompensas obtenidas por el staking de dicho ether, menos las penalizaciones aplicadas a los validadores.

Para realizar el proceso inverso, es decir, recuperar el ether depositado, se procede a quemar una cantidad equivalente de stETH, lo cual generalmente resulta en una conversión 1:1 entre stETH y ether.

Un ejemplo para poder entender cómo funciona la relación entre stETH y wstETH:

El usuario convierte ("wrappea") 1 stETH en su versión tokenizada y obtiene 0.9803 wstETH. Este proceso, conocido como "wrappear" (o encapsular), se refiere a la conversión de un activo en una versión tokenizada que puede ser utilizada en una red blockchain diferente. En este caso, el activo original, stETH, se "envuelve" en un contrato inteligente, creando un token equivalente (wstETH) que mantiene el valor del activo subyacente. Si ocurre un rebase y el precio de wstETH sube, por ejemplo, un 5%, el usuario puede desenvolver esos 0.9803 wstETH que había obtenido inicialmente y recibir 1.0499 stETH, ya que ahora 1 stETH equivale a 0.9337 wstETH.

6. Integración y uso de stETH y wstETH en DeFi

Estos tokens, compatibles con los estándares ERC-20, han sido ampliamente adoptados en todo el ecosistema DeFi, gracias a su capacidad para integrarse en diversas capas de la arquitectura descentralizada. DeFi utiliza una arquitectura de múltiples capas, donde cada una tiene un propósito específico y construye sobre las anteriores, creando una infraestructura abierta y altamente componible que permite a cualquiera desarrollar, reutilizar o interactuar con otras partes del ecosistema (Schär, 2019).

En esta estructura, las capas son jerárquicas y su seguridad depende de la solidez de las capas inferiores. Por ejemplo, si la blockchain en la capa de liquidación (Layer 1) se ve comprometida, todas las capas subsecuentes también estarían en riesgo. De manera similar, si se utilizara un libro mayor con permisos como base, cualquier esfuerzo de descentralización en las capas superiores sería ineficaz (Schär, 2019).

Las principales capas de esta arquitectura son:

- **Capa de liquidación (Layer 1):** Consiste en la blockchain y su activo nativo (por ejemplo, BTC en la blockchain de Bitcoin y ETH en la blockchain de Ethereum). Esta capa permite que la red almacene de manera segura la información de propiedad y asegura que cualquier cambio de estado cumpla con las reglas establecidas. La blockchain sirve como la base para la ejecución sin confianza y actúa como capa de liquidación y resolución de disputas.
- **Capa de activos (Layer 2):** Incluye todos los activos emitidos sobre la capa de liquidación. Esto abarca tanto el activo nativo del protocolo como cualquier otro activo adicional que se emita en esta blockchain, comúnmente referidos como tokens.
- **Capa de protocolos (Layer 3):** Proporciona estándares para casos de uso específicos como exchanges descentralizados, mercados de deuda, derivados y gestión de activos en cadena. Estos estándares se implementan generalmente como un conjunto de contratos inteligentes a los que cualquier usuario o aplicación DeFi puede acceder, haciendo que estos protocolos sean altamente interoperables.
- **Capa de aplicaciones (Layer 4):** Crea aplicaciones orientadas al usuario que se conectan a protocolos individuales. La interacción con los contratos inteligentes se abstrae generalmente mediante una interfaz web, lo que facilita el uso de los protocolos.
- **Capa de agregación (Layer 5):** Es una extensión de la capa de aplicaciones. Los agregadores crean plataformas centradas en el usuario que se conectan a varias aplicaciones y protocolos.

Suelen proporcionar herramientas para comparar y calificar servicios, permiten a los usuarios realizar tareas complejas conectándose a varios protocolos simultáneamente, y combinan la información relevante de manera clara y concisa.

Dentro de esta estructura, los tokens de Lido, como stETH, se integran principalmente en la capa de protocolos (Layer 3) y aplicaciones (Layer 4), donde pueden ser utilizados en diversas estrategias financieras, como en pools de liquidez y protocolos de préstamos, ampliando la eficiencia y flexibilidad del ecosistema DeFi.

6.1 Liquidity pools

Los liquidity pools, o fondos de activos en criptomonedas mantenidos en contratos inteligentes, son la base del intercambio en los mercados descentralizados. Los usuarios proporcionan sus activos a estos fondos y, a cambio, reciben una parte de las comisiones generadas por las transacciones realizadas en el pool. Estos conjuntos de tokens permiten intercambios fluidos entre diferentes criptomonedas mediante el uso de creadores de mercado automatizados (AMM). Un AMM, en resumen, es un mecanismo utilizado por los exchanges descentralizados que permite a los usuarios conectar sus billeteras y realizar intercambios de tokens sin la necesidad de intermediarios centralizados.

El stETH, que representa el ETH depositado para staking, puede intercambiarse por ETH convencional dentro de uno de estos pools de liquidez. Además, stETH puede utilizarse para intercambiarse por otros tokens, no solo por ETH, sino por cualquier otro token que tenga una pool de liquidez existente.

La principal ventaja de utilizar pools de liquidez descentralizados radica en la eliminación del requisito de confianza hacia un intermediario centralizado. Según Schär (2019), los exchanges centralizados, aunque eficientes, presentan riesgos significativos, ya que los usuarios deben depositar sus activos en la plataforma y confiar en el operador del exchange, lo que expone sus fondos a posibles pérdidas por mal manejo o ataques externos. En contraste, los protocolos de intercambio descentralizado, como los AMM, permiten a los usuarios mantener el control de sus activos hasta que se ejecuta la transacción, lo que mitiga el riesgo de contraparte y evita la necesidad de intermediarios.

En los AMM, los precios de los tokens en los liquidity pools se determinan generalmente mediante un modelo de producto constante, que ajusta el precio relativo de los tokens en función de la relación entre las reservas de los tokens en el contrato inteligente. Este modelo asegura que los pools de liquidez no pueden agotarse, ya que el precio de un token aumenta a medida que disminuyen sus reservas (Schär, 2019). Además, este sistema permite la

acumulación de fondos adicionales en el pool, beneficiando a los proveedores de liquidez que reciben tokens de participación en el pool a cambio de su contribución, lo que les permite acceder a su parte proporcional del pool creciente.

Un ejemplo destacado de la implementación de este modelo es Curve, una plataforma optimizada para intercambiar stablecoins con bajas fluctuaciones de precio. Otros ejemplos incluyen UniSwap, Balancer y Bancor, todos los cuales utilizan variantes del modelo de producto constante para garantizar la eficiencia y liquidez en el intercambio de tokens.

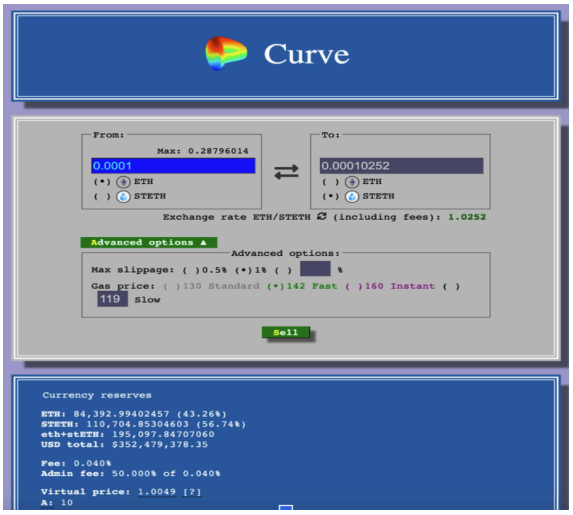


Figura 6. Imagen de como se ve Curve.

6.2 Préstamos

Los protocolos de préstamos en el ecosistema DeFi permiten a los usuarios pedir prestados activos utilizando stETH como colateral. Para lograr esto, es necesario envolver el stETH, lo que lo convierte en un activo aplicable como garantía. Este proceso no solo facilita los préstamos, sino que también abre una capa adicional de eficiencia y composabilidad dentro del ecosistema DeFi, especialmente en estrategias como el yield farming. Esta estrategia consiste en optimizar el rendimiento de las inversiones depositando activos en diversas plataformas o protocolos para obtener las mayores recompensas posibles. Ejemplos de protocolos que han adoptado stETH como colateral incluyen Aave, Maker, Compound, Cream y Alpha.

Los protocolos de préstamos en DeFi se destacan por ser completamente permissionless, es decir, no requieren que el prestatario o el prestamista se identifiquen. Esto permite que cualquier persona tenga acceso a la plataforma y potencialmente pueda pedir prestado o proporcionar liquidez para ganar intereses (Schär, 2019). Para proteger al prestamista y evitar que el prestatario se apropie de los fondos sin reembolsarlos, los préstamos suelen estar

completamente garantizados con colateral. El colateral se bloquea en un contrato inteligente y solo se libera una vez que la deuda ha sido pagada.

Además, la fluctuación de los precios del activo colateral subyacente juega un papel crucial en la determinación del factor de salud[2] de un usuario y el riesgo de liquidación. Sin embargo, al utilizar stETH como colateral, los usuarios pueden mejorar constantemente su factor de salud y reducir el riesgo de liquidación a medida que se acumulan las recompensas de staking.

Los protocolos de préstamos también permiten el préstamo de stETH, lo que podría permitir a los usuarios tomar un préstamo que se paga de manera constante a sí mismo gracias a las recompensas generadas. Si hay una gran demanda de stETH prestado, los proveedores también pueden ganar recompensas adicionales en su stETH.

Schär (2019) señala que existen diferentes tipos de plataformas de préstamos descentralizadas, como los mercados de deuda colateralizada y los mercados de deuda colateralizada por pares (P2P). En estos sistemas, los préstamos están completamente garantizados por el colateral, que se bloquea en un contrato inteligente hasta que se devuelve la deuda. Este enfoque elimina la necesidad de intermediarios centralizados y permite una mayor flexibilidad y eficiencia en el uso del capital dentro del ecosistema DeFi.

6.3 Estrategias/Agregadores

Los agregadores pueden usar stETH en sus estrategias de yield farming como una capa adicional de recompensas encima de su ya existente estrategia. Las mismas son flexibles y pueden maximizar las recompensas más altas posibles para sus usuarios. Ejemplos populares de agregadores incluyen: Yearn, Harvest, Badger.

Estas estrategias pueden utilizar una variedad de otros protocolos e iniciativas para generar altas recompensas, como el yield farming a través de incentivos de liquidity mining. Este último es un proceso en el cual los usuarios proporcionan liquidez a un protocolo o plataforma a cambio de recompensas, típicamente en forma de tokens adicionales. También incluyen ganar recompensas a través de protocolos de préstamos (como se discutió anteriormente), obtener beneficios mediante el staking en protocolos nativos, y así sucesivamente.

[2] Métrica utilizada en protocolos de préstamos descentralizados para evaluar la seguridad de una posición de préstamo o colateral. Representa la relación entre el valor de tus colaterales y el valor de tus préstamos, ajustado por los ratios de colateralización específicos de cada activo.

stETH en Harvest Finance. Un ejemplo de estrategia existente es el pool de liquidez stETH-ETH, que aprovecha las recompensas de liquidity mining generadas al proporcionar liquidez en el pool Curve stETH-ETH. Estas recompensas se reinvierten automáticamente en stETH y ETH, que luego se utilizan para aumentar la participación en el mismo pool.

Con la adición de protocolos de préstamos que adoptan stETH como colateral, los usuarios pueden implementar nuevas estrategias utilizando los activos obtenidos. Por ejemplo, es posible proporcionar stETH como garantía, pedir prestado, y usar esos activos para oportunidades de yield farming como proporcionar liquidez en pools como Curve o Onsen, o incluso para pedir prestada una nueva posición y continuar optimizando retornos.

Utilizar stETH/wstETH como colateral en DeFi es beneficioso por varias razones:

1. Son casi tan seguros como el ether en términos de precio. Exceptuando escenarios catastróficos, su valor tiende a mantener una relación 1 a 1 contra ether.

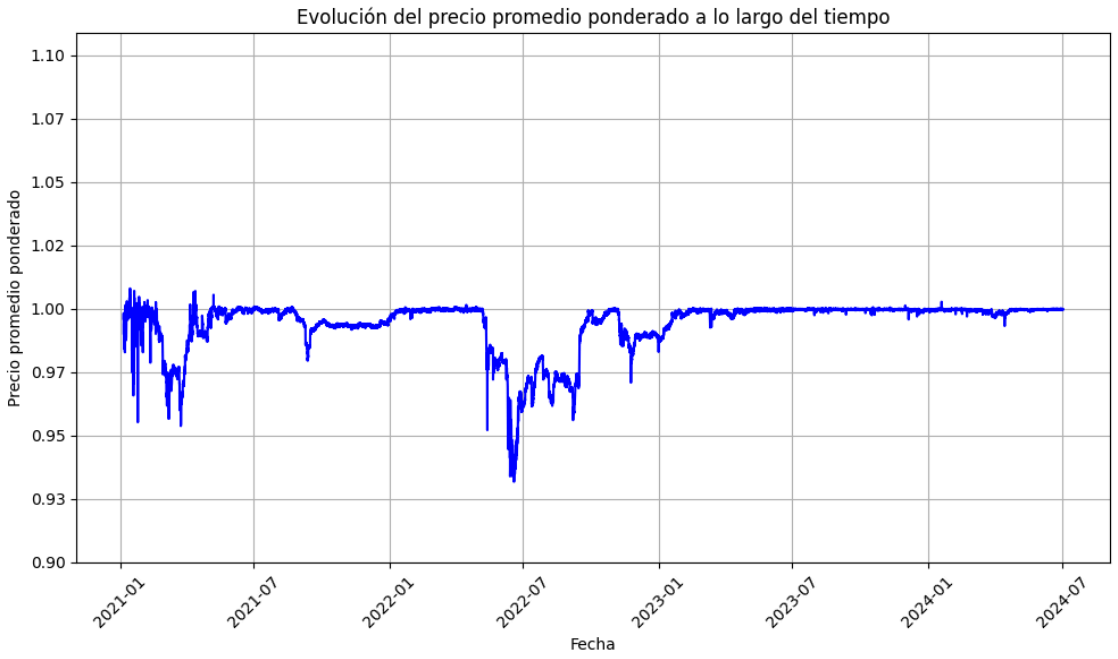


Figura 7. Fuente: https://dune.com/LidoAnalytical/Curve-ETHstETH

En este gráfico se puede ver el valor histórico de la relación entre stETH y ETH, el peor valor fue en julio 2022 llegando a 0.94 ETH por cada stETH aproximadamente, habiendo recuperado posteriormente el peg, y manteniéndose estable desde 2023.

2. Obtener recompensas sobre el colateral efectivamente reduce el costo del préstamo.
3. Son tokens bastante líquidos con miles de millones en depósitos.

Respecto a exchanges descentralizados, stETH se encuentra listado en algunos de los más importantes:

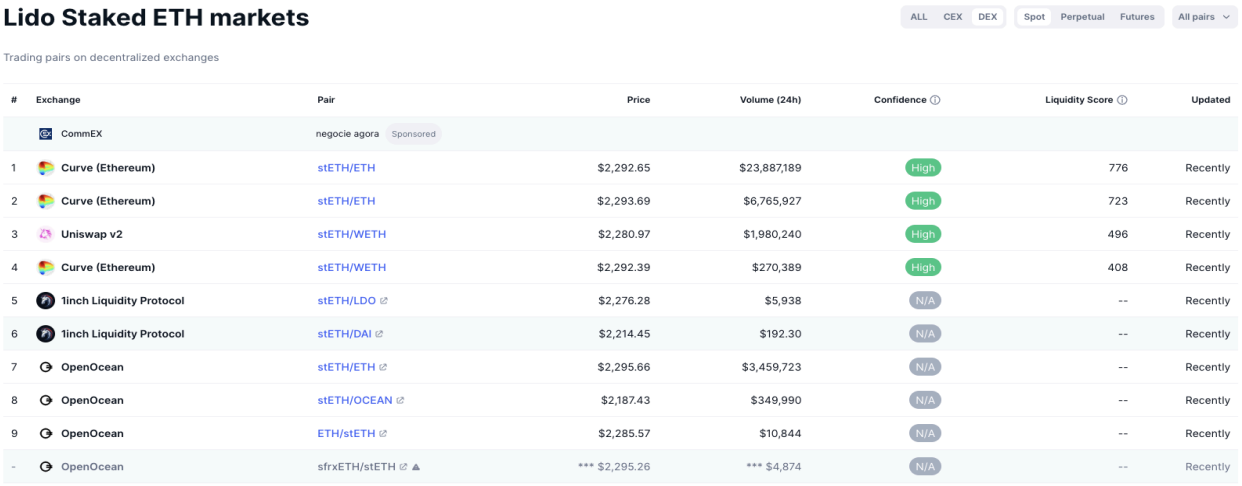
1. Uniswap
2. Curve
3. Balancer
4. SushiSwap
5. CowSwap

Dado esto, resulta sumamente importante mencionar y explicar qué son estos protocolos. Los exchange descentralizados (DEX) surgen ofreciendo autonomía y seguridad en el espacio criptográfico, a diferencia de sus contrapartes centralizadas, los DEX no están regidos por entidades soberanas, sino que operan bajo la lógica de contratos inteligentes. Básicamente actúan como facilitadores P2P, es decir, intercambio entre personas sin ningún intermediario, permitiendo que las transacciones fluyan entre ellos. Acá los usuarios tienen control absoluto sobre sus claves privadas, y por ende de sus criptomonedas.

Esto posee dos grandes riesgos, el primero es no ser responsable de las llaves de la billetera, ya que en caso de pérdida es irrecuperable. Y además, el riesgo de hackeos, ya que los contratos inteligentes no son infalibles y hay muchos hackers en el ecosistema buscando cómo explotar fallas en los mismos.

Cabe destacar que los DEX en general son complejos, no tienen la mejor experiencia de usuario, y a veces depende la blockchain, pueden llegar a tener algunos problemas de liquidez. Por otro lado, su gran ventaja es la anonimidad.

El exchange descentralizado donde más stETH se encuentra depositado es en Curve, dentro de la blockchain de Ethereum, con un volumen operado de 30.5M USD en las últimas 24 hs al 24/12/2023.



Lido Staked ETH markets

ALL CEX DEX | Spot Perpetual Futures | All pairs

Trading pairs on decentralized exchanges

#	Exchange	Pair	Price	Volume (24h)	Confidence ⓘ	Liquidity Score ⓘ	Updated
	CommEX	negocie agora Sponsored					
1	Curve (Ethereum)	stETH/ETH	$2,292.65	$23,887,189	High	776	Recently
2	Curve (Ethereum)	stETH/ETH	$2,293.69	$6,765,927	High	723	Recently
3	Uniswap v2	stETH/WETH	$2,280.97	$1,980,240	High	496	Recently
4	Curve (Ethereum)	stETH/WETH	$2,292.39	$270,389	High	408	Recently
5	1inch Liquidity Protocol	stETH/LDO	$2,276.28	$5,938	N/A	--	Recently
6	1inch Liquidity Protocol	stETH/DAI	$2,214.45	$192.30	N/A	--	Recently
7	OpenOcean	stETH/ETH	$2,295.66	$3,459,723	N/A	--	Recently
8	OpenOcean	stETH/OCEAN	$2,187.43	$349,990	N/A	--	Recently
9	OpenOcean	ETH/stETH	$2,285.57	$10,844	N/A	--	Recently
-	OpenOcean	sfrxETH/stETH ▲	*** $2,295.26	*** $4,874	N/A	--	Recently

Figura 8. Fuente: https://coinmarketcap.com/currencies/steth/

Podemos ver más datos al momento como la cantidad de stETH depositado en el pool, actualmente es de 50.652 stETH y 48.892 ETH, generando un valor en USD depositado en el pool de $229.121.082.

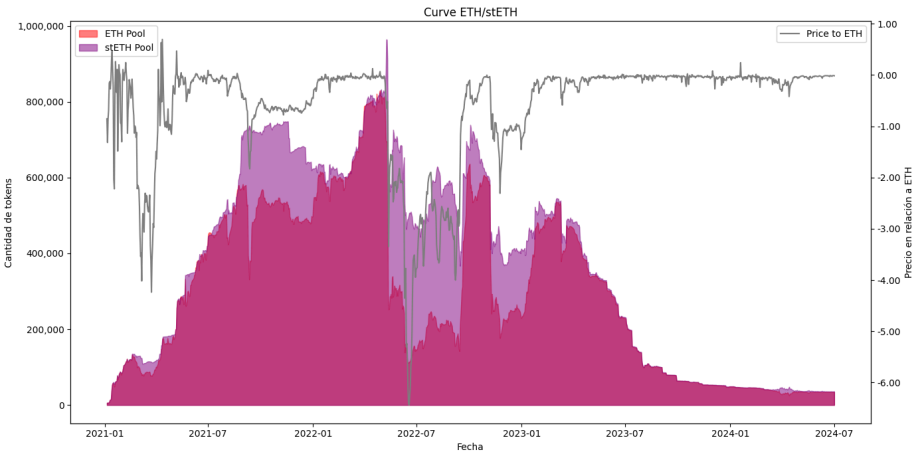


Figura 9. Fuente: https://dune.com/LidoAnalytical/Curve-ETHstETH

En este gráfico se puede ver en rojo, el ether depositado en el pool, en violeta el stETH depositado en el pool, y la línea gris la relación entre el precio de ambos. Puede ser observado y sacar como conclusión que cada vez que el depósito de stETH era mayor que el de ether, la paridad 1 a 1 entre ambos se perdió, llegando a mínimos a mediados de 2022 como previamente fue comentado. A partir de abril 2023 se puede ver que tanto el área roja, como la violeta se mueven en sintonía, la paridad entre ambos está equilibrada. Esto no es menor, ya que la pérdida de peg de stETH puede impactar en liquidaciones, cómo también trae consecuencias a nivel recompensas planeadas por quien deposita ETH para obtener stETH, ya que el gran beneficio del liquid staking es poder ganar con la tasa de interés del token mientras puede ser utilizado en DeFi, pero si el token que se posee pierde valor, el escenario calculado previo al depósito no termina siendo el mismo.

Otro punto a observar respecto a esto, es como mientras que el stETH no pierda el peg, los retiros y depósitos en el pool se mueven medianamente balanceados.

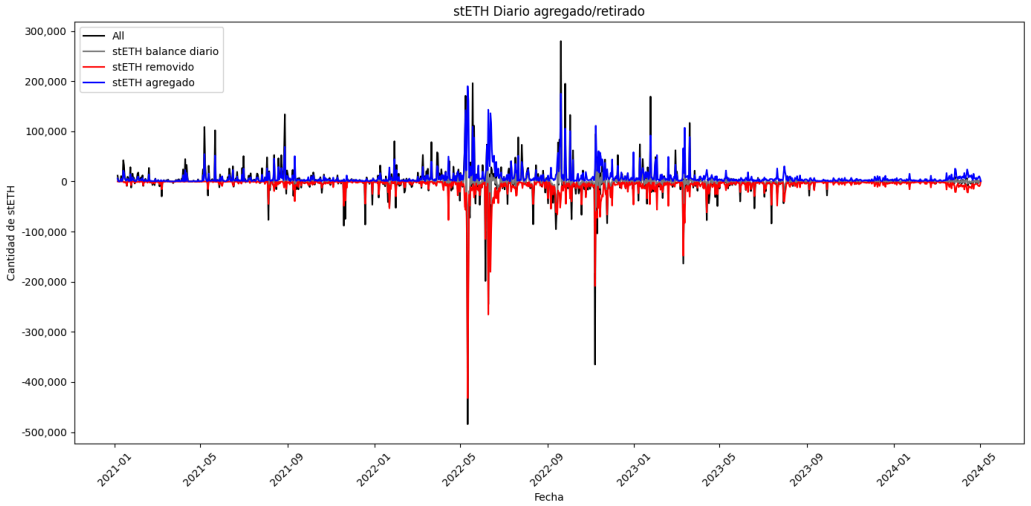


Figura 10. Fuente: https://dune.com/LidoAnalytical/Curve-ETHstETH

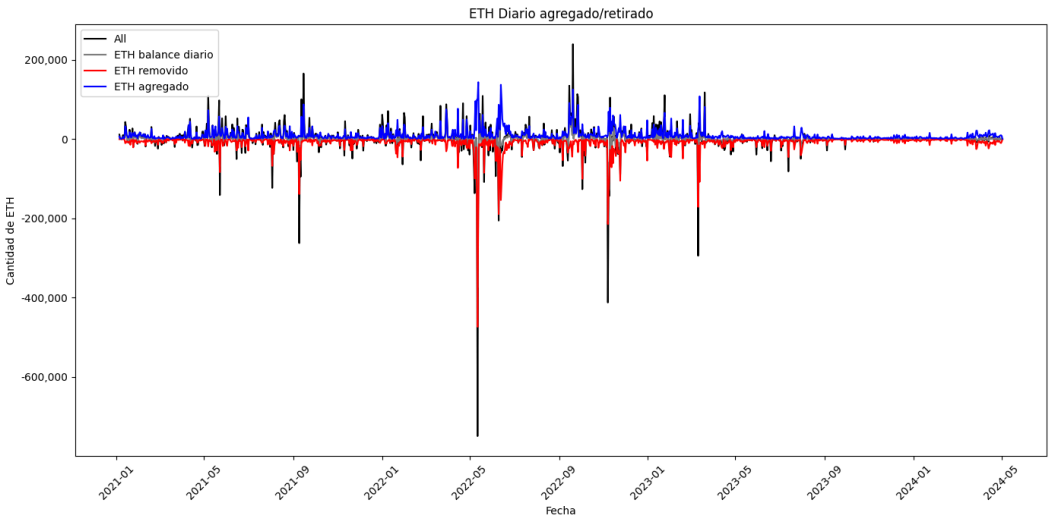


Figura 11. Fuente: https://dune.com/LidoAnalytical/Curve-ETHstETH

Por último, cabe destacar cómo fue variando el valor en USD depositado en este pool con el cambio del valor del ether, llegando a máximos de casi $6.000 M de USD.

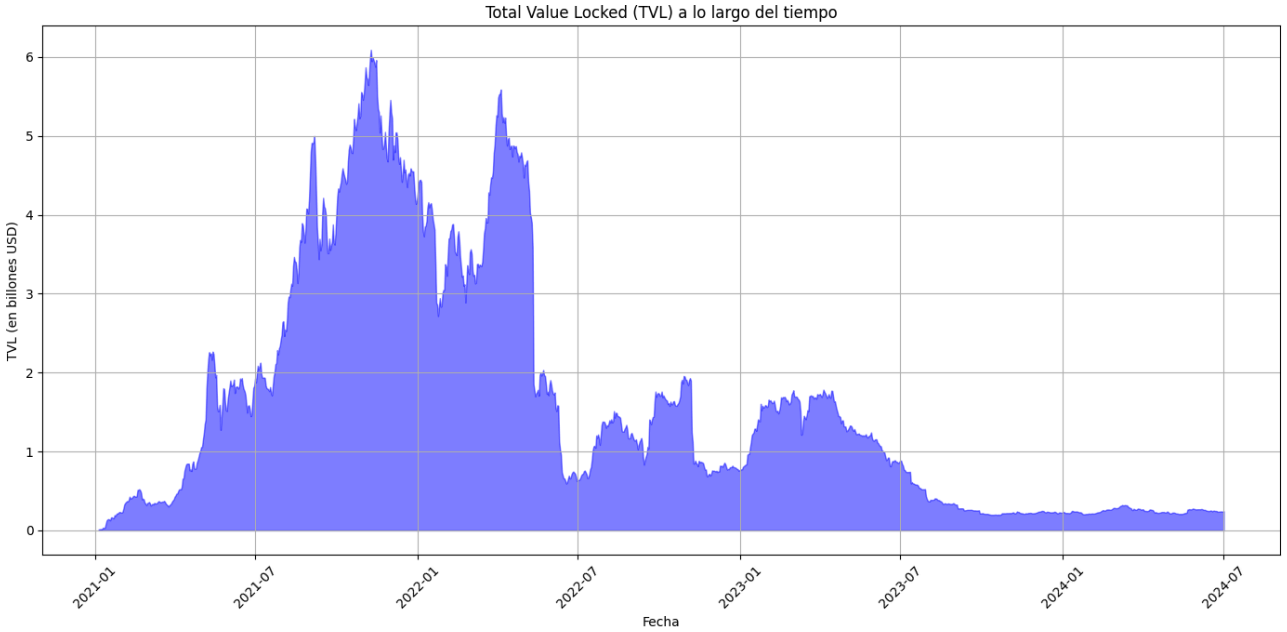


Figura 12. Fuente: https://dune.com/LidoAnalytical/Curve-ETHstETH

Otro de los grandes exchanges descentralizados donde wstEth tiene un gran número de depósitos es en Balancer. Este DEX posee unos 7.000 pools aproximadamente, y $975M USD en depósitos al momento de escribir. El mismo, posee un pool entre WETH y wstETH. En este gráfico podemos observar el histórico de depósitos de estos tokens en el pool.

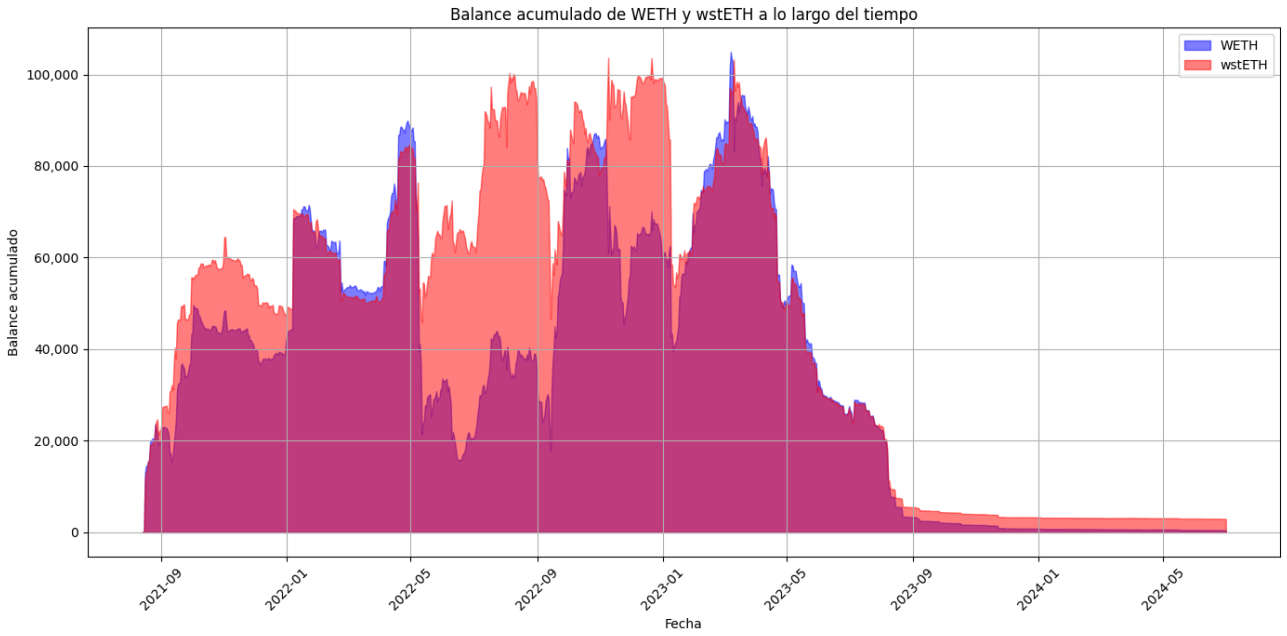


Figura 13. Fuente: https://dune.com/LidoAnalytical/Balancer-WETHwstETH

También puede verse el valor histórico de este par en Balancer llegando a un pico de $527 M USD, teniendo hoy unos 3.291 wstETH y 819 WETH valorizado en $10M USD, eso es aproximadamente un poco más del 1% depositado en todo Balancer.

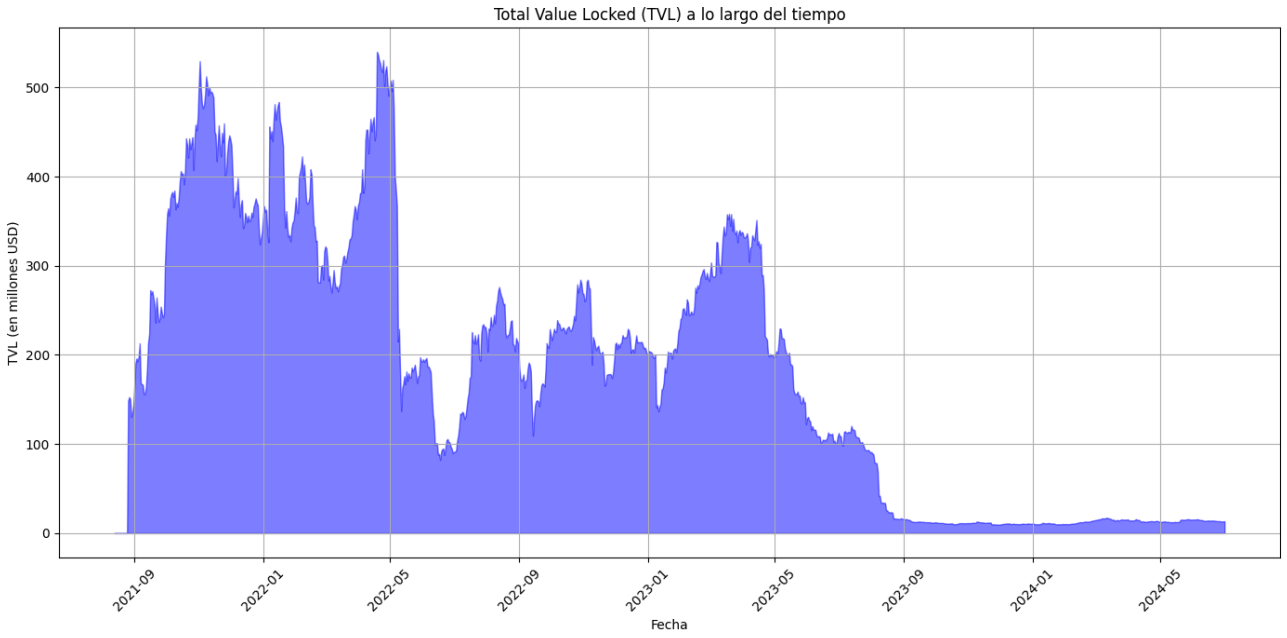


Figura 14. Fuente: https://dune.com/LidoAnalytical/Balancer-WETHwstETH

En el caso de depósitos y préstamos, se pueden encontrar depósitos de stETH o wstETH en:

1. Aave

2. Compound
3. Euler

Estos protocolos son sistemas descentralizados que permiten a los usuarios prestar y tomar prestados activos digitales sin un intermediario en el medio de ambos. A hoy, hay 22.128MM de USD depositados en estos protocolos siendo Aave y Compound de los más grandes, con $6.507MM y $2.361MM respectivamente.

Estos protocolos se basan en la ideología de democratizar el acceso a los servicios financieros, eliminando intermediarios y reduciendo las barreras de entrada. Al operar de manera descentralizada, permiten una mayor inclusión financiera y ofrecen una alternativa a los sistemas bancarios tradicionales, tienen como objetivo proporcionar un sistema en el que los usuarios puedan participar activamente tanto en el suministro como en la toma de préstamos de activos digitales. Fueron creados para solucionar la falta de transparencia, altas comisiones, procesos lentos y acceso restringido que tiene el sistema tradicional, permitiendo así también que los usuarios de DeFi con un exceso de capital, puedan depositar ese dinero en alguno de estos protocolos y obtener rendimientos sobre sus criptomonedas.

Algo clave a entender es que, si una persona necesita tomar un préstamo, ya que requiere, por ejemplo, una cantidad de dinero en dólares para realizar una determinada actividad o compra, como la adquisición de un automóvil, y además posee un activo que no desea vender para mantener la exposición al mismo con la expectativa de que su valor aumente, podría depositarlo en cualquiera de estos protocolos y tomar un préstamo en una moneda que se mueve de manera lineal con el dólar. De esta forma, se bloquean fondos que respaldan la devolución del préstamo solicitado. Cabe mencionar que se paga una tasa de interés por este préstamo, la cual se calcula en función de la utilización del dinero en el protocolo. Por este motivo, es posible encontrar distintas tasas en el mercado, que varían en función de la liquidez que cada protocolo posee.

Entonces, el funcionamiento básico de estos protocolos implica la interacción de dos partes principales, los proveedores de liquidez (depositantes), y los demandantes de liquidez (prestatarios). Los depositantes suministran sus activos a pools de liquidez, y a cambio reciben tokens que representan su participación generando intereses. Por otro lado, los prestatarios toman préstamos de estos pools proporcionando un colateral que garantiza el préstamo.

Como se mencionó previamente, las tasas de interés generalmente son dinámicas, ajustándose según la oferta y la demanda del mercado, lo que asegura un equilibrio entre los activos disponibles para prestar y la correspondiente demanda de préstamos.

Es sumamente importante entender cómo funciona el proceso de colateral. Cuando un usuario solicita un préstamo, este se encuentra sobrecolateralizado, es decir, el valor del colateral supera al del préstamo. Cada activo tiene un factor de colateralización que define qué porcentaje de su valor puede ser prestado. Por ejemplo, si un activo tiene un factor de colateralización del 75% y un usuario deposita un colateral por valor de 10.000 USD, podría obtener un préstamo de hasta 7.500 USD. Los usuarios deben mantener la relación colateral-préstamo dentro de los límites establecidos por el protocolo. Si el valor del colateral disminuye debido a cambios en el mercado, el usuario debe añadir más colateral o reembolsar parte del préstamo para mantener la posición.

Si esto no llega a suceder, es decir, si el valor del colateral cae por debajo de un umbral específico (esto es conocido como relación mínima de colateralización), se activa un proceso de liquidación. De esta forma, el umbral asegura que el colateral pueda cubrir siempre el valor del préstamo teniendo en cuenta la volatilidad que el mercado posee. Cuando se activa una liquidación, una parte o la totalidad del colateral del prestatario se vende en el mercado abierto o se ofrece a liquidadores a un precio con descuento. Estos liquidadores son participantes del mercado que reembolsan una parte del préstamo a cambio del colateral.

Este proceso protege al protocolo y a los depositantes de la insolvencia, asegura que los préstamos se reembolsen incluso si el prestatario no logra o puede hacerlo, ya que el descuento ofrecido a los liquidadores sirve como un mecanismo de mercado para una respuesta rápida y eficiente ante la caída de valor del colateral. Para los prestatarios resulta clave monitorear constantemente la relación colateral-préstamo en estos mercados para evitar precisamente ser liquidados.

Un ejemplo:
Suponiendo que una persona tiene 1 Bitcoin (BTC) y el precio actual de este es de $40.000. Si desea obtener un préstamo en USDC (una stablecoin cuyo valor es aproximadamente igual a 1 USD) y el factor de colateralización es del 75% para BTC, entonces puede depositar su BTC como colateral en el protocolo, pudiendo retirar hasta un 75% del valor de su BTC como máximo, lo cual equivale a $30.000 USD. Sin embargo, en este caso, solo desea retirar el equivalente a $20.000 USD, ya que la moto que desea comprar tiene ese valor, y esta cantidad está por debajo del máximo permitido.

Para un préstamo de ese monto ($20.000) y un factor de colateralización del 75%, el valor límite de colateral se calcula de la siguiente manera:

Valor de colateral requerido = Monto del préstamo/factor de colateralización

Valor de colateral requerido = 20.000/0.75 = 26.666,67

Esto significa que el factor de salud, que es la relación entre el valor actual del colateral depositado y el valor mínimo requerido para mantener el préstamo, se calcula de la siguiente manera:

Factor de salud = Valor actual del colateral / Valor del colateral requerido

Factor de salud = 40.000/26.666,67 = 150%

Esto indica que el valor actual del colateral es 1.5 veces el valor mínimo necesario para mantener el préstamo y evitar la liquidación, lo que representa una posición relativamente segura contra la liquidación. Si el factor de salud disminuye acercándose a 1, el riesgo de liquidación aumenta.

Con el tiempo, el valor del colateral (en este caso BTC) fluctúa. Si el precio de BTC baja, el valor del colateral también disminuirá.

Supongamos entonces que el precio de BTC cae a $30.000 por BTC; el colateral ahora vale ese mismo monto. Para calcular el valor máximo del préstamo a este nuevo precio, se multiplica el valor por el ratio de colateralización, lo que da como resultado $22.500. Dado que solo se tomó un préstamo de $20.000, la persona se encuentra más cerca de la liquidación, pero aún no es liquidable, recordando que el límite estaba en $26.666,67.

En este caso, existen dos formas de mitigar este riesgo, una es añadir más colateral, sería más BTC para aumentar el valor del colateral depositado. Y la segunda, sería reembolsar una parte del préstamo para disminuir el monto total adeudado.

El factor de salud es esencialmente una medida de seguridad. Cuanto más alto sea este, más segura es la posición del préstamo. Un factor alto indica que el colateral tiene un valor sustancialmente mayor que el monto del préstamo, proporcionando así un colchón contra la volatilidad del mercado.

Continuando con las métricas a hoy, en protocolos de depósito y préstamo, son proporcionados como colateral 3.129.172, estando el 96.4% en ethereum, 2.5% en arbitrum, casi el 1% en optimism, y el resto dividido entre base y polygon.

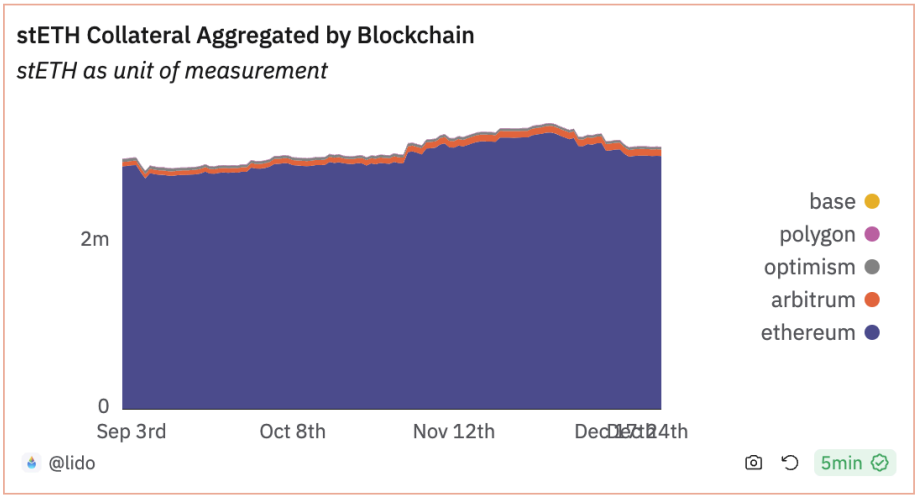


Figura 15. Fuente: https://dune.com/lido/wsteth-as-collateral

Del total de stETH en circulación, el 34.3% está representado como colateral, es decir, los 3.129.172 mencionados anteriormente, habiendo tenido un pico en agosto de 2023 que superó el 40% del total.

Figura 16. Fuente: https://dune.com/lido/wsteth-as-collateral

Los montos proporcionados como colateral se encuentran divididos en varios protocolos, en su gran mayoría en ethereum mainnet como ya se mencionó anteriormente. Al realizar una foto a la fecha, los principales protocolos se llevan el 88% aproximadamente :

1. Aave V3. 29.28%
2. Maker. 28.19%
3. Spark. 16.8%
4. Aave V2. 13.78%.

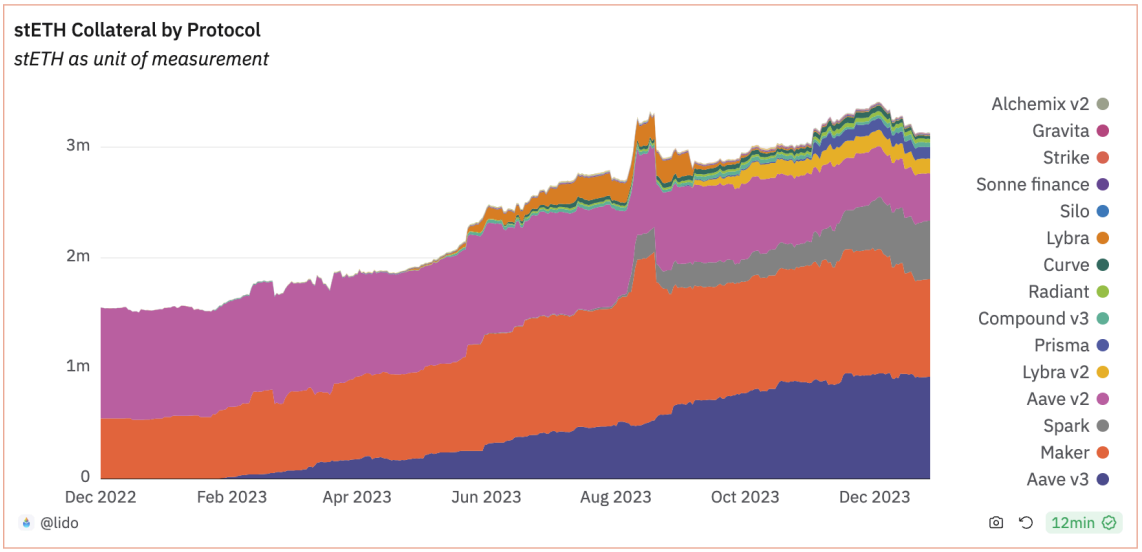


Figura 17. Fuente: https://dune.com/lido/wsteth-as-collateral

Respecto a liquidaciones, en la imagen debajo puede ser observado en violeta el número de liquidaciones, es decir, la cantidad, y en rojo el monto medido en stETH. El promedio para el último mes de noviembre fue un 0.47 cantidad de liquidaciones diarias, y un monto promedio de 2.87 stETH liquidados.

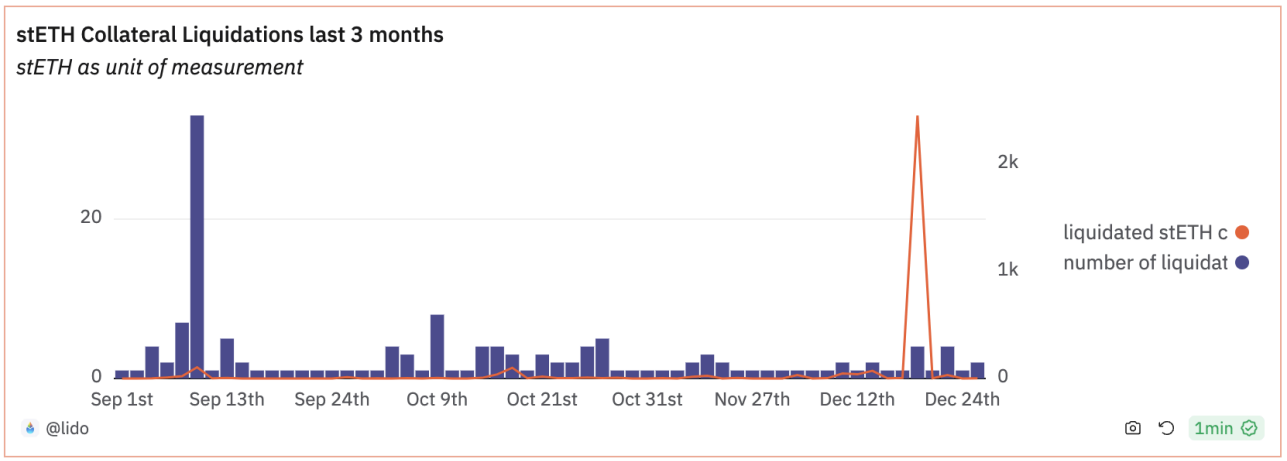


Figura 18. Fuente: https://dune.com/lido/wsteth-as-collateral

Si se desean observar las liquidaciones desde otra perspectiva, se pueden analizar por protocolo, es decir, en qué protocolo ocurrieron más liquidaciones y contra qué activo. En los últimos 3 meses, el protocolo donde se registró el mayor número de liquidaciones fue Curve. La razón principal es que el 18 de diciembre se produjo una liquidación significativamente mayor que el promedio, con un monto de 2,477.2 stETH, de los cuales 2,455.04 corresponden a Curve y 7.82 stETH a liquidaciones en Aave V2.

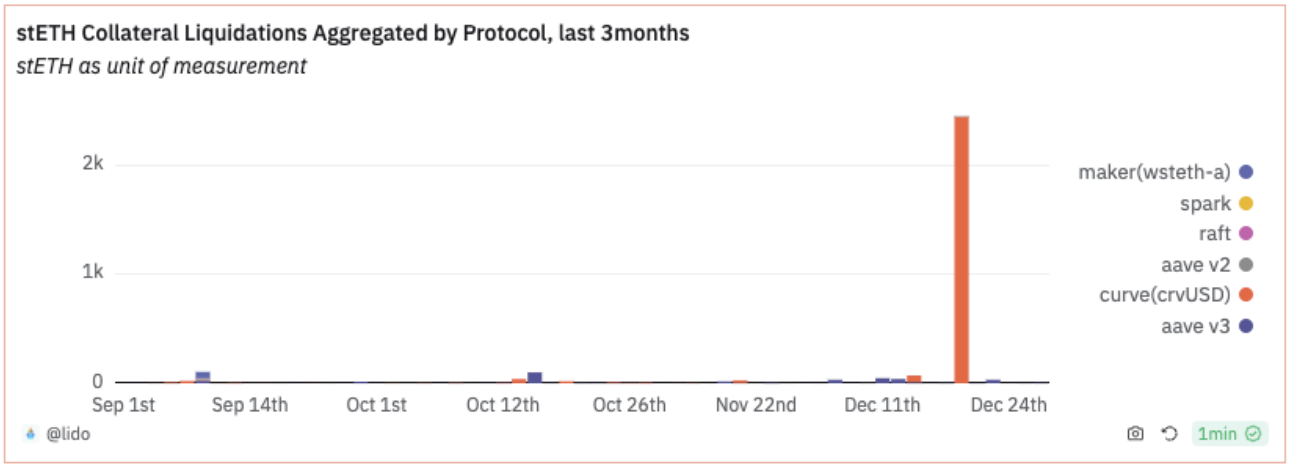


Figura 19. Fuente: https://dune.com/lido/wsteth-as-collateral

Esa liquidación mayor fue contra un token del protocolo Curve (crvUSD), lo que explica que un gran porcentaje de las liquidaciones de ese día ocurrieron en ese protocolo.

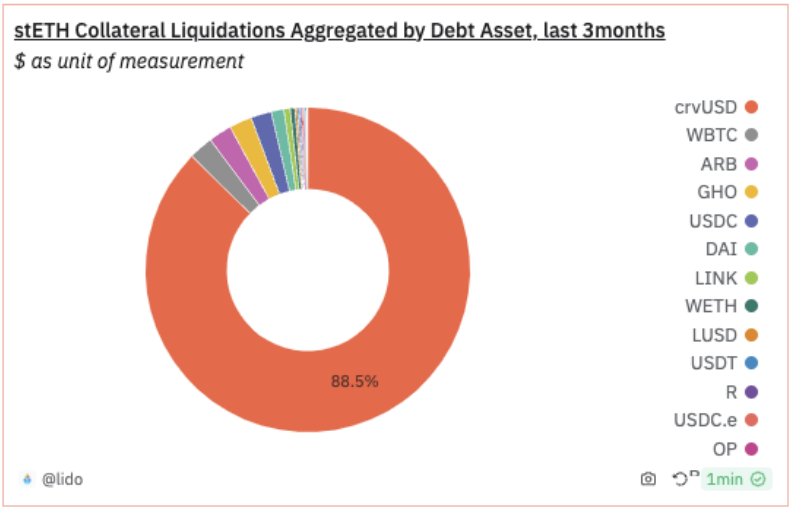


Figura 20. Fuente: https://dune.com/lido/wsteth-as-collateral

MakerDAO

Otro de los grandes protocolos que utiliza wstETH como colateral es MakerDAO. Su creación principal, DAI, es una criptomoneda estable (stablecoin) cuyo valor se mantiene anclado al dólar estadounidense, diseñada para ofrecer estabilidad en un ecosistema conocido por su volatilidad. La gobernanza en MakerDAO es un ejemplo de democracia descentralizada; los poseedores de MKR toman decisiones vitales, desde ajustar las tasas de estabilidad hasta aprobar nuevos tipos de colaterales, asegurando que cada cambio refleje la voluntad colectiva de su comunidad.

DAI frente a otras stablecoins

Si bien existen otras stablecoins ampliamente utilizadas como USDT (Tether) y USDC (USD Coin), DAI se distingue por ser descentralizada y por su mecanismo de emisión basado en el bloqueo de criptoactivos como colateral. Mientras que USDT y USDC son emitidas por entidades centralizadas que respaldan sus tokens con reservas de moneda fiduciaria, DAI se genera a través de contratos inteligentes en la blockchain de Ethereum, utilizando activos digitales como ETH y wstETH como garantía.

Esta diferencia es crucial en el contexto de las finanzas descentralizadas (DeFi), ya que DAI permite a los usuarios participar en el ecosistema sin depender de intermediarios centralizados, alineándose con los principios fundamentales de DeFi. El proceso de colateralización para generar DAI implica bloquear criptoactivos en "Vaults" (bóvedas), lo que no es posible con stablecoins centralizadas como USDT y USDC.

Importancia de DAI en el uso de wstETH como colateral

La elección de DAI en este análisis se debe a que su modelo de emisión ilustra cómo wstETH puede ser utilizado como colateral para crear una stablecoin descentralizada. Al integrar wstETH, MakerDAO permite a los usuarios obtener liquidez en forma de DAI sin necesidad de vender sus participaciones en staking, proporcionando acceso a fondos y manteniendo la exposición a ETH.

Estabilidad y mecanismos de control

La estabilidad de DAI se logra mediante un sistema adaptable de tasas de interés y mecanismos de liquidación. Las tasas de estabilidad se ajustan en respuesta a las fluctuaciones del mercado, equilibrando la oferta y demanda del token y asegurando su paridad con el dólar. Cuando el valor de los colaterales cae peligrosamente, se activan mecanismos de liquidación que protegen a DAI de la volatilidad del mercado.

El Dai Savings Rate (DSR) es otro componente clave que permite a los usuarios ganar intereses sobre sus tokens, incentivando el ahorro y contribuyendo a mantener el "peg" con el dólar. Este mecanismo no está presente en las stablecoins centralizadas, donde los usuarios no pueden influir en la emisión ni en las políticas monetarias. Básicamente, es una herramienta que incentiva a los usuarios a mantener el token; al depositar Dai en una cuenta especial, los usuarios ganan un porcentaje de interés sobre sus fondos, el cual se genera en Dai.

Cuando el DSR aumenta, se vuelve más atractivo para los usuarios ahorrar Dai, lo que reduce la cantidad de Dai en circulación y puede ayudar a aumentar su valor si está por debajo de su paridad con el dólar. Inversamente, reducir el DSR puede estimular a los usuarios a gastar o invertir su Dai, aumentando la oferta en el mercado y potencialmente reduciendo su valor si está sobrevalorado.

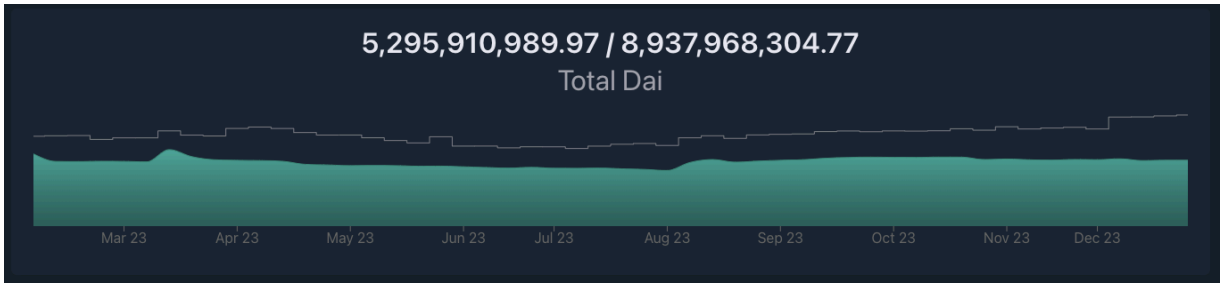


Figura 21. Fuente: https://daistats.com/#/overview

El Dai total muestra la cantidad del token existente (la cantidad de liquidez disponible para usuarios, comerciantes y ahorradores), seguido por la cantidad máxima actual permitida para ser generada. Todo el suministro de Dai se genera a partir de una creciente cantidad de activos colaterales.

Los tipos de colateral solo se agregan al Protocolo Maker cuando son aprobados por los tenedores de tokens MKR, quienes votan a través de un proceso de gobernanza descentralizada. Algunos tipos de colaterales tienen dos variaciones: A y B, que permiten a los usuarios generar Dai a partir de estos activos bajo diferentes conjuntos de parámetros de riesgo (es decir, techos de deuda, tasas de estabilidad, ratios de liquidación y penalizaciones por liquidación). Por ejemplo:

- ETH-A permite generar hasta 590 millones de Dai con una Tasa de Estabilidad del 2% y un Ratio de Liquidación del 150%.
- ETH-B permite generar hasta 15 millones de Dai con una Tasa de Estabilidad del 4% y un Ratio de Liquidación del 130%.

ETH-A ofrece una gran cantidad de liquidez a una tasa baja, mientras que ETH-B tiene tasas más altas, pero un ratio de liquidación más bajo. Esto les da a los usuarios la opción de generar más Dai de su colateral de lo que permite ETH-A, pero con un mayor riesgo de liquidación.

La aceptación de wstETH como colateral por parte de MakerDAO tiene varias implicaciones y beneficios:

- **Diversificación de colateral:** Al aceptar wstETH, MakerDAO diversifica los tipos de activos que respaldan la emisión de DAI, lo que puede ayudar a mejorar la estabilidad y la resistencia de su sistema.
- **Integración con el staking de Ethereum:** Al integrar wstETH, MakerDAO se vincula directamente con el ecosistema de staking de Ethereum, permitiendo a los usuarios de staking participar en DeFi sin necesidad de liquidar su posición en stETH.
- **Liquidez y Acceso:** Los usuarios de Lido pueden usar su wstETH como colateral para obtener DAI, lo que proporciona liquidez y acceso a fondos sin necesidad de vender sus participaciones en staking.
- **Incentivos y Riesgos:** Aceptar wstETH como colateral también implica ciertos riesgos, como la volatilidad del valor de stETH/wstETH y la dependencia del buen funcionamiento de Lido y del mecanismo de staking de Ethereum.

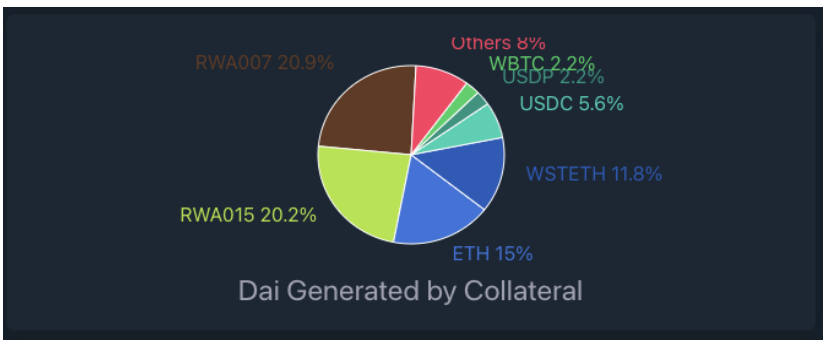


Figura 22. Fuente: https://daistats.com/#/overview

Del total de 5,295,910,989.97 de Dai generados al momento de escribir, el 11.8% es con wstETH como colateral, dividido en dos vaults, wstETH-A y wstETH-B.

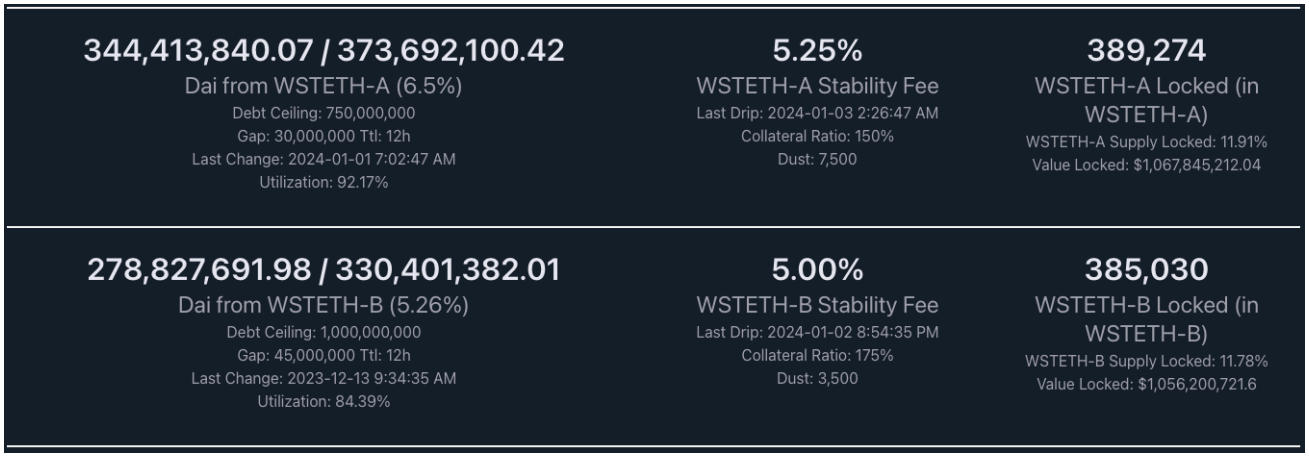


Figura 23. Fuente: https://daistats.com/#/overview

Un total de 344M de Dai fueron creados con el vault A, y otros 278M de Dai con el vault B. La principal diferencia entre ambos es que el ratio de colateral para el primero es de 150%, y 175% para el segundo. Actualmente, hay 389K wstETH depositados en el A, y otros 385K en el B. A lo largo del tiempo, el depósito de wstETH en estos vaults fue cambiando, como puede ser observado en la imagen debajo:

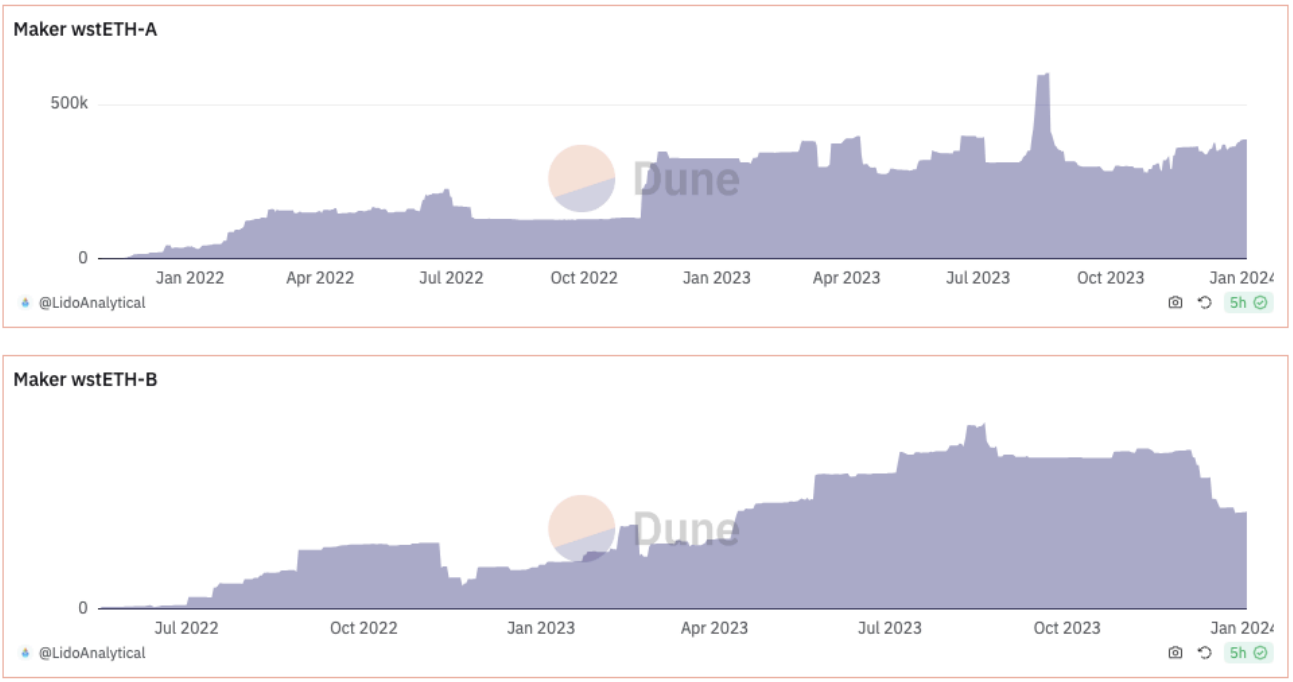


Figura 24. Fuente: https://dune.com/lido/wsteth-as-collateral

Rebases Diarios y Mecanismo de Participaciones

Normalmente, los rebases de stETH ocurren diariamente cuando el oráculo[3] de Lido informa sobre la actualización del saldo de ether en la cadena Beacon. El rebase puede ser positivo o negativo, dependiendo del rendimiento de los validadores. En caso de que los validadores de Lido sean penalizados o sancionados, los saldos de stETH pueden disminuir de acuerdo con el tamaño de la penalización.

Por lo tanto, los rebases diarios resultan en cambios en los saldos de tokens stETH, este mecanismo se implementa mediante participaciones (shares).

Por lo tanto, la participación es una unidad básica que representa la porción del titular de stETH en el total de ether controlado por el protocolo. Cuando ocurre un nuevo depósito, se emiten nuevas participaciones para reflejar qué porción del ether controlado por el protocolo se añadió al fondo. Cuando llega el informe del oráculo de la Beacon, el precio de las participaciones en stETH es recalculado, las mismas no están normalizadas, por lo que el contrato también almacena la suma de todas las participaciones para calcular el saldo de tokens de cada cuenta.

El saldo de participaciones por el saldo de stETH puede calcularse con esta fórmula:

$$Shares[account] = balanceOf(account) * totalShares / totalPooledEther$$

[3] Los oráculos actúan como puentes que suministran datos del mundo real a los contratos inteligentes, permitiendo que estos se ejecuten en función de eventos o condiciones externas.

7. Riesgos

Riesgos actuales

Seguridad de contratos inteligentes: Existe un riesgo inherente de que Lido pueda contener una vulnerabilidad o error en su contrato inteligente. El código del protocolo es público, fue auditado y está cubierto por un extenso programa de recompensas por errores para minimizar este riesgo.

Riesgo técnico de la cadena Beacon: Lido está construido sobre tecnología experimental en desarrollo activo, y no hay garantía de que la Cadena Beacon haya sido desarrollada sin errores. Cualquier vulnerabilidad inherente en la cadena conlleva riesgos de penalización (slashing) y fluctuación en el saldo de stETH.

Riesgo de penalización (slashing): Los validadores de la cadena Beacon arriesgan penalizaciones de staking, con hasta el 100% de los fondos apostados en riesgo si fallan. Para minimizar este riesgo, Lido se inclina por múltiples operadores de nodos profesionales y reputados con configuraciones heterogéneas, con mitigación adicional en forma de auto-cobertura.

Riesgo del precio de stETH: Los usuarios corren el riesgo de que el precio de intercambio de stETH sea menor que su valor intrínseco, lo que hace posible el arbitraje y termina siendo un mercado con ciertos riesgos.

La DAO de Lido está orientada a mitigar los riesgos mencionados y eliminarlos en la medida de lo posible. A pesar de esto, estos riesgos pueden seguir existiendo.

Comparativa entre el análisis de 2022 y el análisis Actual

En 2022, Lido Finance realizó un análisis exhaustivo para evaluar los riesgos asociados al slashing dentro del protocolo, utilizando las especificaciones de Phase 0 y Altair durante las fases iniciales de la transición de Ethereum 2.0. El análisis actual, en contraste, se basa en la especificación Capella, que representa una fase más avanzada de Ethereum 2.0. Esta actualización introduce mejoras significativas en la precisión y severidad de las penalizaciones por slashing, lo que permite una evaluación más precisa y alineada con las condiciones actuales de la red.

- **Enfoque en penalizaciones por slashing**

El análisis de 2022 abordó los riesgos de slashing para operadores de nodos grandes, evaluando escenarios en los que hasta el 100% de los validadores bajo su control podrían ser penalizados. En contraste, el análisis actual se enfoca en una variedad de escenarios con porcentajes específicos de validadores slasheados (0.0495%, 10%, 15%, 20%). Esta diversidad de escenarios permite una

evaluación de riesgos más detallada y precisa, adaptándose mejor a la realidad actual de la red Ethereum y al comportamiento de los validadores en un entorno más maduro.

- **Resultados y capacidad de respuesta financiera**

En cuanto a la evaluación de la capacidad de Lido para mitigar las pérdidas por slashing, el análisis actual proporciona un enfoque más detallado sobre cómo el protocolo podría utilizar sus recursos financieros actuales, incluyendo fondos de seguro y reservas en stETH, DAI y USDT. A diferencia del análisis de 2022, que se centró principalmente en el uso de ingresos proyectados a cinco años, el modelo actual considera la respuesta inmediata a escenarios de slashing utilizando los recursos disponibles, lo que ofrece una visión más práctica y realista de la resiliencia financiera de Lido.

Conclusión de la comparativa

En resumen, el análisis actual, basado en la especificación Capella y adaptado a los escenarios más probables de slashing, ofrece una evaluación más actualizada y precisa de los riesgos que enfrenta Lido.

8.¿Qué son los validadores?

Los validadores son nodos especiales en la red de Ethereum que participan activamente en el proceso de consenso. A diferencia de los mineros en el mecanismo Proof of Work (PoW), los validadores no requieren de gran poder computacional. En su lugar, participan en el proceso de validación y creación de bloques mediante el bloqueo de una cantidad específica de Ether (ETH). Este bloqueo sirve como un compromiso y una garantía de su honestidad en el proceso. Cada validador representa un bloqueo inicial de 32 ETH.

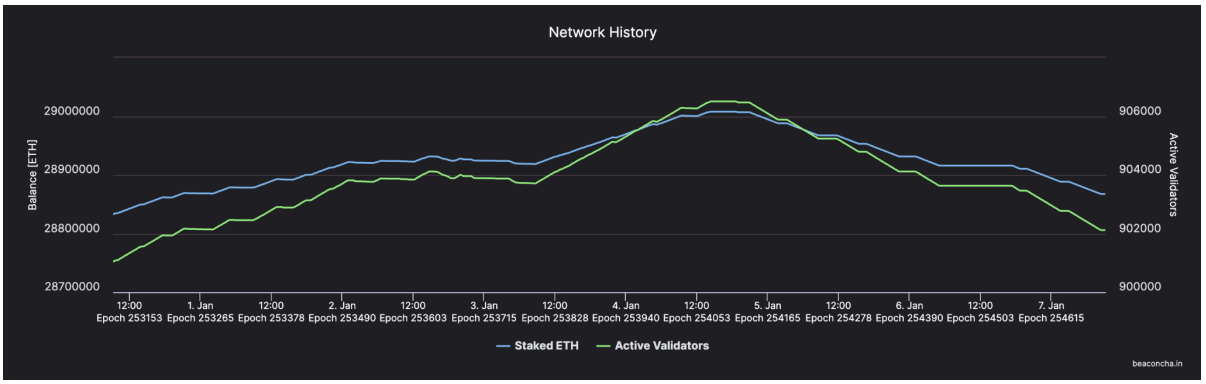


Figura 25. Fuente: https://beaconcha.in/charts

Los validadores tienen algunas funciones clave:

- **Proponer bloques.** Los validadores tienen la responsabilidad de proponer nuevos bloques para la blockchain. En cada epoch, uno de los validadores es seleccionado de manera pseudoaleatoria para ser el block proposer (proponente del bloque). Este validador reúne las transacciones de la red y crea un bloque que luego debe ser validado por otros validadores.
- **Validar y votar (Attestations).** Para cada bloque propuesto, los validadores deben realizar attestations, que son votos acerca de la validez del bloque propuesto y del estado de la cadena de bloques. Este proceso asegura que el bloque siga las reglas del protocolo y que los validadores verifiquen de manera conjunta el estado actual de la blockchain.

  Los validadores que no son seleccionados para proponer un bloque en un slot determinado participan en este proceso de attestations, validando la propuesta del block proposer.

- **Formar parte de comités.** Durante cada epoch, los validadores se dividen en comités, que están encargados de realizar las attestations en un slot específico. Cada comité tiene un número de validadores que participan en la validación de bloques.
- **Agregación de attestations.** Algunos validadores dentro de un comité son seleccionados para ser attestation aggregators, cuya función es recoger y organizar las attestations enviadas por los

demás validadores, asegurando que al menos 2/3 de los validadores del comité aprueben un bloque antes de que este sea finalizado y agregado a la blockchain.

- **Finalizar transacciones.** Los validadores aseguran que las transacciones en la red sean finalizadas, lo que significa que no pueden ser revertidas sin un coste altísimo o una probabilidad bajísima. Esto refuerza la seguridad de la red y la inmutabilidad de las transacciones una vez que se ha alcanzado la finalidad, lo cual ocurre aproximadamente cada 12 minutos (2 epochs).

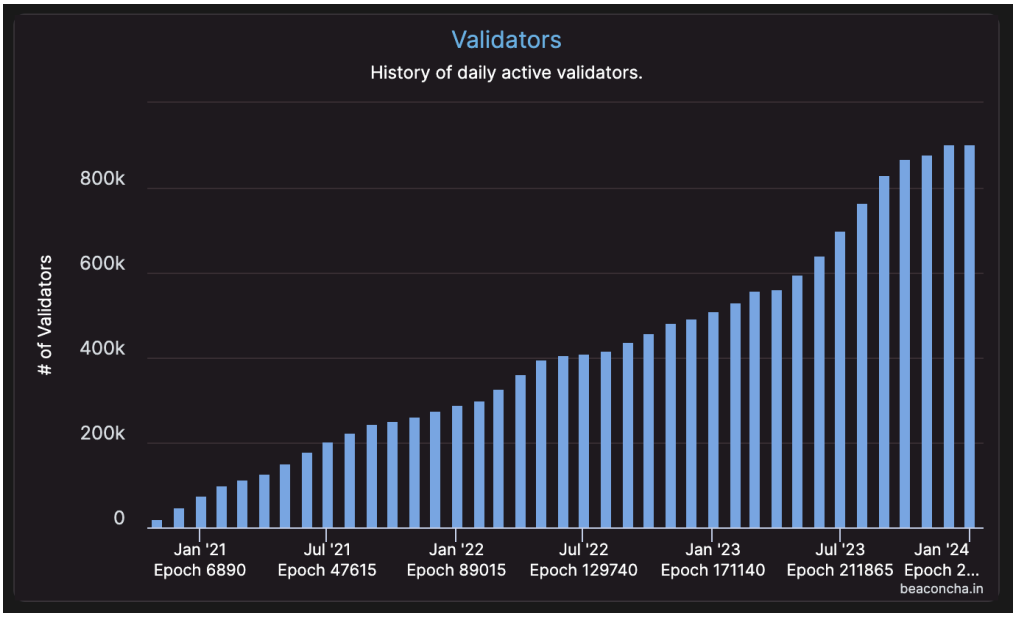


Figura 26. Fuente: https://beaconcha.in/charts

La existencia de validadores es fundamental para el funcionamiento de los modelos PoS. Como fue mencionado anteriormente, la seguridad de la red no depende de la capacidad computacional, como en PoW, sino de la cantidad de moneda que los validadores están dispuestos a bloquear. Este cambio responde a la necesidad de una mayor eficiencia energética y escalabilidad.

9. El rol de los nodos

Un nodo en la red Ethereum es esencialmente un participante que posee una copia completa o parcial de la cadena de bloques. Estos nodos cumplen varias funciones críticas:

1. **Almacenamiento de datos**

   Cada nodo almacena información sobre el estado actual de la red, incluyendo todas las transacciones y bloques.

2. **Procesamiento de transacciones**

   Los nodos participan en la verificación y procesamiento de transacciones. Esto incluye verificar la validez de las transacciones según las reglas del protocolo Ethereum.

3. **Conservación de la cadena de bloques**

   Los nodos mantienen y actualizan la cadena de bloques, agregando nuevos bloques a medida que son validados y aceptados en la red.

4. **Comunicación en la red**

   Los nodos se comunican entre sí para transmitir información, como transacciones y bloques nuevos, asegurando que todos los nodos estén sincronizados.

Existen diferentes tipos de nodos, como nodos completos, nodos ligeros y nodos de archivo, cada uno con su propio conjunto de responsabilidades y requisitos de almacenamiento.

Nodos completos

Su responsabilidad principal es verificar todas las transacciones y bloques en la cadena, ejecutando todas las reglas del protocolo para mantener la red segura y consistente. Almacenan toda la cadena, esto incluye cada transacciones que ocurrieron desde el inicio de la red hasta cada momento actual.

Respecto a sus requerimientos, requieren una cantidad significativa de almacenamiento, ya que deben mantener una copia completa de la cadena, este requisito de almacenamiento está en constante aumento ya que la cadena de bloques crece más y más.

Nodos ligeros

Los nodos ligeros no descargan la cadena de bloques completa, sino que dependen de los nodos completos para obtener la información necesaria. Son sumamente útiles para usuarios que necesitan interactuar con la red sin el almacenamiento o recursos computacionales para mantener un nodo

completo. Un ejemplo de uno de estos puede ser que pueden verificar la validez de la información (como el saldo de una cuenta). Respecto a sus requisitos, requieren mucho menos que los completos, y son ideales para dispositivos con recursos limitados como pueden ser celulares o pequeños servidores privados/personales.

Nodos de archivo

Al igual que los nodos completos, los nodos de archivo almacenan toda la cadena de bloques y verifican todas las transacciones y bloques. Además, mantienen un registro completo del "estado" histórico de la red, esto incluye el estado de cada cuenta en cada bloque pasado, los mismos son esenciales para desarrolladores y servicios que necesitan acceder al estado histórico completo de la red.

Requieren una cantidad masiva de almacenamiento, mucho mayor que los nodos completos, debido a que almacenan no sólo la cadena de bloques, sino también el historial completo de estados de la red.

Algunos puntos que existen entre los nodos y validadores, es decir, la relación entre ambos son que los validadores, que son responsables de proponer y validar bloques en el modelo PoS, están vinculados a nodos específicos. Un nodo puede alojar desde ningún validador hasta cientos o miles de ellos.

Los validadores que están conectados al mismo nodo no actúan de manera independiente. En cambio, comparten la misma "visión" del estado de la red, lo que significa que tienen un entendimiento coherente y sincronizado de la cadena de bloques y sus transacciones.

Aunque los validadores son claves en el proceso de formación de consenso, son los nodos los que realizan la validación efectiva de los bloques y transacciones. Los validadores proponen y atestiguan los bloques, pero la verificación final y la incorporación a la cadena de bloques es realizada por los nodos.

Esta relación entre nodos y validadores es crucial para mantener la seguridad y descentralización de la red Ethereum. Los nodos aseguran que la cadena de bloques sea precisa y resistente a ataques maliciosos, mientras que los validadores garantizan un proceso de consenso eficiente y equitativo.

10. Distribución de los validadores a hoy

En este sistema, se distinguen principalmente dos categorías: ‘Entidades’ y 'Node Operators' (NOs).

Las entidades se definen como la capa de custodia/activos del staking. Son esencialmente agrupaciones de activos (en este caso, ETH) de diferentes participantes. Los pools permiten a los individuos participar en el staking sin necesitar operar un nodo completo, al depositar sus activos a través de un pool compartido. En cambio, los Node Operators (NOs) son operadores de nodos donde su función es operar los nodos que efectivamente participan en el proceso de consenso de la red. Estos nodos pueden ser responsables de validar transacciones y bloques, y su operación es crucial para mantener la seguridad y estabilidad de la red.

Cada operador de nodo, es responsable de operar un nodo o varios en la red, estos nodos a su vez están vinculados con validadores específicos. En resumen, los operadores de nodos son los que proporcionan la plataforma y las condiciones necesarias para que los validadores puedan operar eficientemente en la red.

En total existen 40 entidades al día de hoy, las cuáles son:

1. Lido
2. Coinbase
3. Binance
4. RocketPool
5. Kraken
6. OKex
7. Bitcoin Suisse
8. Ledger Live
9. Whale 0x5d76a
10. Frax
11. Celsius Network
12. Swell
13. CoinSpot
14. Octant
15. StakeWise
16. SSV
17. BitStamp
18. StakeHound
19. Stader-PermissionLess
20. Stader-Permissioned
21. KuCoin
22. Ether Capital
23. Bitfinex
24. Ankr
25. Wexexchange
26. Bitpie
27. BTC-e
28. Paxos
29. CoinDCX
30. Fireblocks
31. Vitalik Buterin
32. Enzyme
33. Bake.io
34. Guarda
35. StaFi
36. SharedStake
37. Hord.fi
38. Bifrost
39. pStake
40. Komainu

Fuente: https://www.rated.network/?network=mainnet&view=pool&poolType=all&timeWindow=1d&page=1

Siendo 14 de ellos exchange centralizados.

El siguiente gráfico muestra el porcentaje de validadores que tiene cada entidad sobre el total de validadores en Ethereum. Se puede ver que solamente Lido posee aproximadamente el 32% de los validadores, lo cual representa hoy un gran riesgo de centralización, esto podría llevar a una

vulnerabilidad en la red, tanto desde un punto de vista técnico (fallos comunes) como político (influencia desmedida en la toma de decisiones).

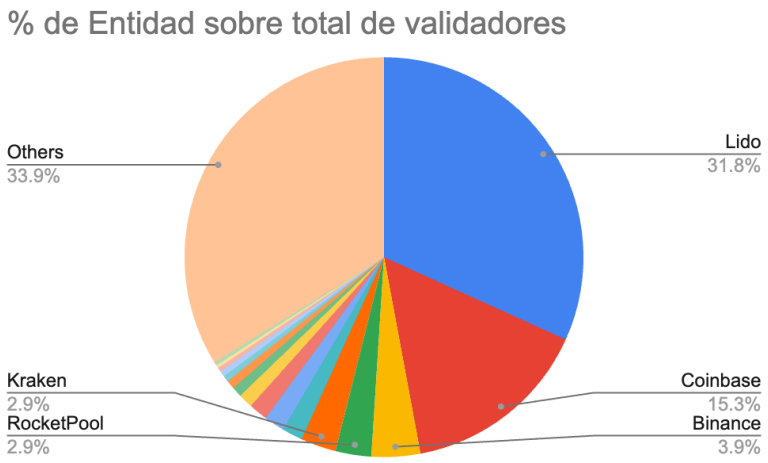


Figura 27. Distribución de entidad sobre validadores

Si examinamos la composición de Lido, este es el listado de operadores de nodo que posee actualmente, es decir, al día de hoy:

1. Kukis Global
2. Stakely
3. Nethermind
4. Attestant
5. Prism Team at Offchain
6. Blockdaemon
7. HashQuark
8. CryptoManufaktur
9. Sigma Prime
10. ChainSafe
11. Stakin
12. Simply Staking
13. BridgeTower
14. Figment
15. Everstake
16. ChainLayer
17. RockX
18. Allnodes
19. DSRV
20. P2P.ORG - P2P Validator
21. Consensys
22. Chorus One
23. Blockscape
24. Kiln
25. RockLogic GmbH
26. Stakefish
27. Staking Facilities
28. SenseiNode
29. Ebunker
30. RockawayX Infra
31. A41
32. Numic
33. ParaFi
34. Launchnodes
35. Gateway.fm

Fuente: https://www.rated.network/o/Lido?network=mainnet&timeWindow=1d&viewBy=operator&page=1

Cada operador de nodos en Lido posee una cierta cantidad de validadores. La cantidad actual de validadores que Lido posee actualmente es de 288.000 aproximadamente distribuído entre los siguiente operadores (Fuente).

Operador de Nodo	# Validadores	% validadores sobre Lido	% validadores sobre totalidad
Kukis Global	9,994	3.46%	1.10%
Stakely	9,994	3.46%	1.10%
Nethermind	9,994	3.46%	1.10%
Attestant	9,994	3.46%	1.10%
Prysm Team at Offchain	9,994	3.46%	1.10%
Blockdaemon	9,994	3.46%	1.10%
HashQuark	9,994	3.46%	1.10%
CryptoManufaktur	9,994	3.46%	1.10%
Sigma Prime	9,994	3.46%	1.10%
ChainSafe	9,994	3.46%	1.10%
Stakin	9,994	3.46%	1.10%
Simply Staking	9,539	3.31%	1.05%
BridgeTower	9,085	3.15%	1.00%
Figment	9,085	3.15%	1.00%
Everstake	9,085	3.15%	1.00%
ChainLayer	9,085	3.15%	1.00%
RockX	8,903	3.09%	0.98%
Allnodes	8,903	3.09%	0.98%
DSRV	8,903	3.09%	0.98%
P2P.ORG - P2P Validator	8,903	3.09%	0.98%
Consensys	8,903	3.09%	0.98%
Chorus One	8,903	3.09%	0.98%
Blockscape	8,813	3.05%	0.97%
Kiln	8,813	3.05%	0.97%
RockLogic GmbH	8,540	2.96%	0.94%
Stakefish	8,540	2.96%	0.94%
Staking Facilities	8,449	2.93%	0.93%
SenseiNode	6,996	2.42%	0.77%
Ebunker	5,996	2.08%	0.66%
RockawayX Infra	5,542	1.92%	0.61%
A41	4,815	1.67%	0.53%
Numic	4,815	1.67%	0.53%
ParaFi	4,815	1.67%	0.53%
Launchnodes	2,544	0.88%	0.28%
Gateway.fm	545	0.19%	0.06%

En este caso, se observa el porcentaje que representan los validadores de Lido sobre la totalidad de validadores, alcanzando un total del 31.75%, con una concentración máxima de 3.46% entre los validadores de Lido, que suman un total de 9.994 validadores.

En cuanto a los validadores slasheados hasta la fecha, se registran un total de 408 casos. Esto puede observarse en el siguiente enlace, siendo el primero registrado el 2 de diciembre de 2020.

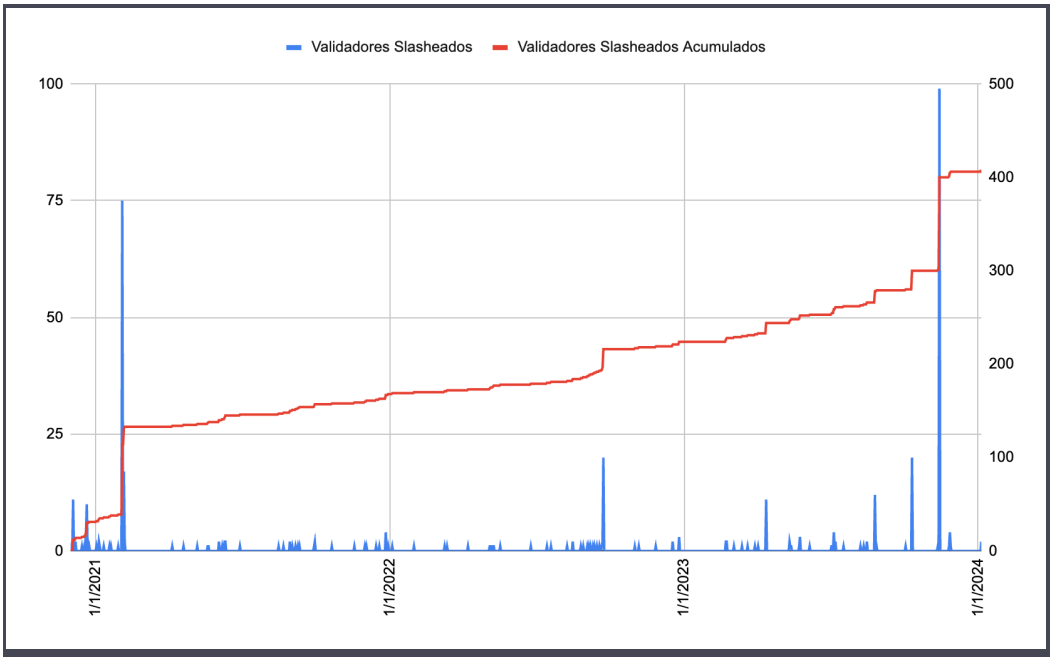


Figura 28. Evolución de los validadores slasheados.

Hasta el momento hubo dos eventos de slashing a validadores de Lido, el primero[4] tuvo que ver con el operador de nodos RockLogic GmgH el 13 de abril de 2023 afectando a 11 validadores. Básicamente se originó por la duplicación de claves de validadores en dos clusters diferentes, lo que derivó en votaciones dobles. Este problema fue causado por un error en la base de datos del cliente de la capa de ejecución y una falla en la actualización y reinicio del cliente Prysm, terminó provocando la reimportación inesperada de claves de validadores eliminadas previamente.

Las penalizaciones iniciales ascendieron aproximadamente hasta 11.1945 ETH, incluyendo penalizaciones por desconexión de todo el cluster durante la investigación. El total de la pérdida terminó siendo de 13.77 ETH.

RockLogic respondió al incidente apagando el cluster de 1,000 validadores y eliminando el cliente de la capa de consenso (Prysm) para evitar el almacenamiento de datos clave, mensajes en cola y datos de nodos. Posteriormente, reactivaron con éxito 989 validadores sin incidentes adicionales. Además,

[4] https://research.lido.fi/t/slashing-incident-involving-rocklogic-gmbh-validators-april-13-2023/4399

solicitó a Lido DAO que utilizara su fondo de cobertura para compensar a los stakers por los daños ocasionados, esto fue aprobado y ejecutado el 30 de junio (tx)[5].

El segundo incidente sucedió el 11 de octubre de 2023. Los colaboradores de la DAO de Lido alertaron al operador de nodos LaunchNodes sobre un evento de slashing que estaba teniendo lugar, afectando a 20 de los validadores operados por ellos. La causa de este suceso se debió a la ejecución de procedimientos de respaldo no óptimos durante problemas de conectividad en el centro de datos. En un intento de restaurar la conectividad de los validadores, se dirigieron a múltiples instancias del cliente validador (una instancia inicial y una instancia de respaldo activada manualmente). Esto causó votos dobles para los validadores cargados.

La pérdida inicial fue 1 ETH de penalización por validador slasheado, y tras el incidente LaunchNodes cerró múltiples clusters que sumaban 2,582 validadores para asegurar que esto no siga ocurriendo, eliminó los clientes y datos originales de los nodos. Terminaron reactivando 2,562 validadores[6].

[5] Se puede obtener más información sobre este suceso en este link.

[6] Se puede obtener más información sobre este suceso en este link.

11. Análisis de escenarios

En cuanto a los riesgos, uno de los más significativos es el que puede ser ocasionado por los slashings, que es el riesgo de que stETH pierda la paridad (peg) que posee con ETH. Para mitigar este riesgo, Lido contrató anteriormente una cobertura de seguros vendida por Unslashed Finance, la cual estuvo vigente hasta 2021.

El problema con esta cobertura era su alto costo, ya que se financiaba con fondos del tesoro de la DAO y representaba el 25% de su rendimiento anual. Debido a esto, Lido decidió crear un fondo de cobertura propio para cubrir los siniestros asociados a este riesgo.

Lido cobra un porcentaje de las recompensas de staking; esta comisión es definida por la DAO y puede ser modificada en el futuro mediante votaciones dentro de la misma. Actualmente, la comisión es del 10%, lo que significa que de cada recompensa de staking, Lido retiene ese porcentaje, del cual la mitad se destina a los operadores de los nodos y la otra mitad al tesoro del protocolo.

Con esta estructura, se puede entender cómo Lido financia el fondo de cobertura mencionado, utilizando básicamente el 5% de las recompensas de staking de sus usuarios. La dirección de este fondo es pública y se encuentra en la siguiente billetera:

https://etherscan.io/address/0x8B3f33234ABD88493c0Cd28De33D583B70beDe35

Actualmente, Lido posee 6,287 stETH depositados en el fondo de cobertura. Cabe destacar que cualquier pérdida que exceda el fondo creado será socializada entre todos los depositantes de Lido (quienes depositaron ETH).

El modelo utilizado para la simulación de pérdidas en el protocolo de Lido se basa en una serie de inputs clave que permiten estimar las posibles pérdidas por slashing y por validadores fuera de línea. A continuación, se explican en detalle los principales inputs utilizados y el razonamiento detrás de su selección.

Estimación de inputs

El estimador principal para calcular las pérdidas por slashing y por validadores fuera de línea se basa en el balance promedio y el balance efectivo de los validadores de Lido. El balance efectivo, que en este caso es de 32 ETH por validador (máximo efectivo), es el valor que determina la cantidad de ETH que puede estar en riesgo en caso de penalización.

Ecuaciones que gobiernan la simulación

El modelo incluye varias ecuaciones clave para calcular las pérdidas debido a slashing y validadores fuera de línea. Estas ecuaciones determinan las pérdidas en stETH y el impacto de esas pérdidas en los fondos de Lido.

1. Pérdida total debido a slashing:

$$Pérdida\ por\ slashing\ =\ (Validadores\ slasheados\ *\ Balance\ efectivo\ del\ validador)$$

2. Pérdida total debido a validadores fuera de línea (penalizaciones por inactividad):

$$Pérdida\ por\ offline\ =\ \frac{Base\ Reward\ *\ (Total\ de\ Epochs\ Fuera\ de\ Línea)}{Número\ de\ validadores\ fuera\ de\ línea}$$

Donde la Base Reward es:

$$Base\ Reward\ =\ \frac{Balance\ efectivo}{\sqrt{Total\ de\ balance\ activo}}\ *\ Base\ reward\ factor$$

3. Proporción de pérdida sobre los depósitos de Lido:

$$\%\ de\ depósitos\ =\ \frac{Pérdida\ total}{Depósitos}\ *\ 100$$

4. Proporción de pérdida sobre los fondos de cobertura de Lido:

$$\%\ de\ fondos\ =\ \frac{Pérdida\ total}{Reservas}\ *\ 100$$

5. Frecuencia de slashing:

$$Frecuencia\ de\ slashing\ =\frac{Total\ validadores\ slasheados}{Total\ validadores\ activos}$$

Supuestos

Para elaborar este modelo, se tomaron algunos supuestos para simplificar los posibles escenarios que podrían ocurrir:

1. El modelo se basa en la actualización en la capa de consenso Capella.
2. Se asumen 0 retiros de ETH depositados hasta este momento.
3. Se supone que la cadena Beacon[7] no entra en modo de fuga (esto significa que la cadena está funcionando de manera estable).

[7] Es la capa de consenso que la blockchain posee en este caso.

4. Los validadores sancionados (slashed) de Lido son los únicos validadores sancionados en la cadena.
5. No se analizan los validadores desconectados ni las penalizaciones.
6. Se asume que 32 ETH es el saldo promedio de los validadores de Lido.
7. Aunque Lido está desplegado en otras cadenas, por razones de impacto se decidió realizar este análisis únicamente para Ethereum.

Elementos exógenos en el ejercicio

El análisis asume que ciertos parámetros son exógenos y no se ven afectados por las decisiones del modelo. Estos incluyen:

- Precio de ETH: Se fija en $2,600 por ETH para los escenarios analizados.
- Políticas de slashing de Ethereum: Las reglas de penalización por slashing son determinadas por el protocolo y no dependen de las acciones de Lido o de sus usuarios.

Análisis de sensibilidad

A continuación, se presentan algunos primeros análisis y escenarios sobre el máximo monto de pérdida que Lido podría afrontar:

1. Escenario 1. Lido enfrenta la pérdida de los validadores solamente con el fondo de seguro que posee.
2. Escenario 2. Lido utiliza además de los fondos del escenario 1, el 80% de los fondos que posee en el tesoro de la DAO solamente con el token stETH.
3. Escenario 3. Además de los fondos del escenario anterior, Lido utiliza los DAI y USDT que también posee en el tesoro (siendo estos dos últimos tokens stablecoins con paridad al dólar estadounidense y el riesgo de que pierdan el peg excede este trabajo).

	scenario_1	scenario_2	scenario_3
total active validators	896,311.00	896,311.00	896,311.00
total eligible ETH	28,681,682.00	28,681,682.00	28,681,682.00
Lido's share	0.33	0.33	0.33
Lido's deposits	9,326,604.00	9,326,604.00	9,326,604.00
Lido's reserves	6,287.00	35,867.00	36,990.08
Average effective balance of validators	32.00	32.00	32.00
Average balance of Lido's validators	32.00	32.00	32.00
1% total validators slashed	2,880.00	2,880.00	2,880.00
2% total validators slashed	5,760.00	5,760.00	5,760.00
3% total validators slashed	8,640.00	8,640.00	8,640.00
4% total validators slashed	11,520.00	11,520.00	11,520.00

Figura 29. Datos sobre los escenarios planteados.

En este cuadro se ve entonces los parámetros que ingresan al modelo:

- Total Active Validators: representa la totalidad de validadores en la Beacon Chain.
- Total Eligible ETH: totalidad de ether depositado en la chain.
- Lido's share: proporción que Lido posee sobre los depósitos.
- Lido's deposits: los depósitos.
- Lido's reserves: cuales son los montos con los cuales Lido afrontaría pérdidas en cada caso.
- Average effective balance of validators: balance promedio de ether de los validadores.
- Average balance of Lido's validators: balance promedio en ether de los validadores de Lido.
- Total validators slashed: distintos escenarios sobre cuantos validadores de Lido se verían slasheados.

Se puede observar que, en un escenario donde el 1% de los validadores de Lido sean slasheados, esto representaría 2,880 validadores. Si el porcentaje aumenta al 2%, esto involucraría un total de 5,760 validadores. En los dos últimos casos, los montos serían de 8,640 y 11,520 validadores para un total del 3% y 4% de validadores slasheados, respectivamente.

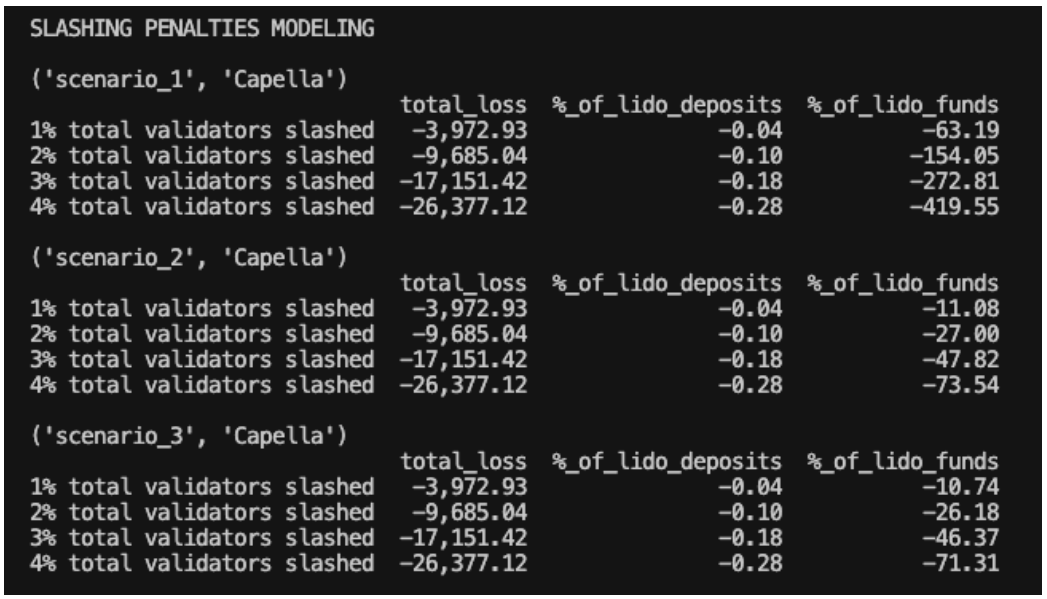
Lido, en este momento, tiene en su fondo de cobertura aproximadamente 6,287 stETH, con lo cual enfrentaría las pérdidas en el escenario 1. En el escenario 2, se plantea que Lido afrontaría las pérdidas tanto con el fondo como con el stETH que posee en su tesoro, que actualmente asciende a 36,975 stETH.

$$\text{Monto escenario 2} = 6{,}287 + 0.8 * 36{,}975 = 35{,}867$$

Para el caso del escenario 3, Lido utiliza lo que posee en el escenario 2, agregando además el 80% de lo que posee en monedas estables lo cual es de $3,650,000.

$$\text{Monto escenario 3} = 6{,}287 + 0.8 * 36{,}975 + 0.8 * (3{,}650{,}000 / 2{,}600) = 36{,}990$$

Siendo el precio promedio de ETH en este momento de $2,600, es necesario analizar las pérdidas en ETH que esto implica.



```
SLASHING PENALTIES MODELING

('scenario_1', 'Capella')
                           total_loss  %_of_lido_deposits  %_of_lido_funds
1% total validators slashed   -3,972.93               -0.04           -63.19
2% total validators slashed   -9,685.04               -0.10          -154.05
3% total validators slashed  -17,151.42               -0.18          -272.81
4% total validators slashed  -26,377.12               -0.28          -419.55

('scenario_2', 'Capella')
                           total_loss  %_of_lido_deposits  %_of_lido_funds
1% total validators slashed   -3,972.93               -0.04           -11.08
2% total validators slashed   -9,685.04               -0.10           -27.00
3% total validators slashed  -17,151.42               -0.18           -47.82
4% total validators slashed  -26,377.12               -0.28           -73.54

('scenario_3', 'Capella')
                           total_loss  %_of_lido_deposits  %_of_lido_funds
1% total validators slashed   -3,972.93               -0.04           -10.74
2% total validators slashed   -9,685.04               -0.10           -26.18
3% total validators slashed  -17,151.42               -0.18           -46.37
4% total validators slashed  -26,377.12               -0.28           -71.31
```

Figura 30. Resultados obtenidos.

Las pérdidas obtenidas en cada escenario serían las mismas, lo que cambiaría serían los montos disponibles con los que Lido las afrontaría. La pérdida medida en stETH para el primer caso es de 3,972 stETH, 9,685 para el segundo caso, 17,151 para el tercero, y, por último, 26,377 para el cuarto. Esto representa el 0.04%, 0.1%, 0.18% y 0.28% sobre los depósitos, respectivamente. Lo importante de este análisis radica en que, si Lido puede afrontar estos montos con los fondos planteados en cada escenario, efectivamente podría hacerlo para todos estos ratios si utiliza fondos de su tesoro. Sin embargo, no podría soportar un 2% de la totalidad de los validadores si se enfrenta a ello solamente con el fondo de seguro.

Por esta razón, se decidió estresar un poco más este análisis, elevando el ratio de validadores posiblemente slasheados.

1. 5%
2. 10%
3. 15%
4. 20%

Esto generaría el siguiente número de validadores slasheados:

1. 14,440
2. 28,880
3. 43,200
4. 57,600

Lo preocupante de esta situación es que Lido, bajo cualquier escenario, no podría cubrir estas pérdidas. Ante un mínimo del 5% del total de los validadores slasheados, utilizando el 80% de sus fondos en el tesoro más el fondo de cobertura, apenas podría equilibrar la pérdida de 37,400 stETH, lo que representaría más del 0.1% del total de ETH depositado en la cadena. En un escenario más extremo, con el 20% de los validadores slasheados, esto representaría aproximadamente el 1.5% del total depositado.

```
SLASHING PENALTIES MODELING

('scenario_1', 'Capella')
                           total_loss  %_of_lido_deposits  %_of_lido_funds
5% total validators slashed   -37,400.88               -0.40           -594.89
10% total validators slashed -119,933.10               -1.29         -1,907.64
15% total validators slashed -249,931.64               -2.68         -3,975.37
20% total validators slashed -429,747.06               -4.61         -6,835.49

('scenario_2', 'Capella')
                           total_loss  %_of_lido_deposits  %_of_lido_funds
5% total validators slashed   -37,400.88               -0.40           -104.28
10% total validators slashed -119,933.10               -1.29           -334.38
15% total validators slashed -249,931.64               -2.68           -696.83
20% total validators slashed -429,747.06               -4.61         -1,198.17

('scenario_3', 'Capella')
                           total_loss  %_of_lido_deposits  %_of_lido_funds
5% total validators slashed   -37,400.88               -0.40           -101.11
10% total validators slashed -119,933.10               -1.29           -324.23
15% total validators slashed -249,931.64               -2.68           -675.67
20% total validators slashed -429,747.06               -4.61         -1,161.79
```

Figura 31. Resultados obtenidos.

Como conclusión, con el fondo que Lido posee, solamente podría cubrir exactamente un 1.45% de los validadores slasheados, un 4.9% en el escenario 2, donde además se utilizan los stETH del tesoro, y un 4.95% en el escenario 3, donde se emplea todo su tesoro al 80% (esto sin considerar lo que se tiene en LDO, el token de Lido).

Para aumentar la conciencia sobre este tema, se decidió realizar simulaciones sobre distintos porcentajes de fondos cubiertos por el tesoro y evaluar cuánto podría ser la pérdida de paridad (depeg) que esto podría generar en stETH en el escenario donde se vean slasheados el 10% del total de los validadores que Lido posee.

Porcentaje de fondos del tesoro	Pérdida de stETH	Reservas			% sobre fondos de Lido		
		Escenario 1	Escenario 2	Escenario 3	Escenario 1	Escenario 2	Escenario 3
25%	119,933	6,287	15,531	15,882	1807.63%	672.23%	655.16%
50%	119,933	6,287	24,775	25,476	1807.63%	384.10%	370.76%
75%	119,933	6,287	34,018	35,071	1807.63%	252.55%	241.97%
80%	119,933	6,287	35,867	36,990	1807.63%	234.38%	224.23%
85%	119,933	6,287	37,716	38,909	1807.63%	217.99%	208.24%
90%	119,933	6,287	39,565	40,828	1807.63%	203.13%	193.75%
95%	119,933	6,287	41,413	42,747	1807.63%	189.60%	180.57%
99%	119,933	6,287	42,892	44,282	1807.63%	179.61%	170.84%

Figura 32. Resultados obtenidos sobre las reservas que Lido posee.

En la sección reservas se fue la cantidad de stETH con el cual se enfrentaría cada escenario para cada porcentaje de los fondos que el tesoro posee, y en la sección % sobre fondos de Lido, cuanto representan las pérdidas sobre estos fondos.

Porcentaje de fondos del tesoro	Total ETH depositado	stETH pérdido + reservas			Total ETH depositado + stETH pérdido		
		Escenario 1	Escenario 2	Escenario 3	Escenario 1	Escenario 2	Escenario 3
25%	9,326,604	-113,646	-104,402	-104,051	9,212,958	9,222,202	9,222,553
50%	9,326,604	-113,646	-95,159	-94,457	9,212,958	9,231,446	9,232,147
75%	9,326,604	-113,646	-85,915	-84,862	9,212,958	9,240,689	9,241,742
80%	9,326,604	-113,646	-84,066	-82,943	9,212,958	9,242,538	9,243,661
85%	9,326,604	-113,646	-82,217	-81,024	9,212,958	9,244,387	9,245,580
90%	9,326,604	-113,646	-80,369	-79,105	9,212,958	9,246,236	9,247,499
95%	9,326,604	-113,646	-78,520	-77,186	9,212,958	9,248,084	9,249,418
99%	9,326,604	-113,646	-77,041	-75,651	9,212,958	9,249,563	9,250,953

Figura 33. Resultados obtenidos sobre las reservas que Lido posee.

En este cuadro se puede observar la pérdida neta que se posee medida en stETH para cada escenario y porcentaje del tesoro post aplicarle la inyección de fondos de cobertura.

Porcentaje de fondos del tesoro	% stETH Depeg		
	Escenario 1	Escenario 2	Escenario 3
25%	-1.22%	-1.12%	-1.12%
50%	-1.22%	-1.02%	-1.01%
75%	-1.22%	-0.92%	-0.91%
80%	-1.22%	-0.90%	-0.89%
85%	-1.22%	-0.88%	-0.87%
90%	-1.22%	-0.86%	-0.85%
95%	-1.22%	-0.84%	-0.83%
99%	-1.22%	-0.83%	-0.81%

Figura 34. Análisis de depeg de stETH por cada escenario.

Cabe destacar el posible depeg que podría generar esto en stETH medido contra ETH, lo que hace que este análisis sea particularmente pertinente. Este depeg podría ser aproximadamente del 1%, sin tener en cuenta las repercusiones psicológicas que esto podría tener, incitando a los depositantes a retirar su ETH, lo que podría generar retiros masivos y una "corrida bancaria".

Importancia de la estimación probabilística del riesgo

Es fundamental no solo calcular la posible pérdida en términos de validadores slasheados, sino también estimar probabilísticamente este riesgo. Para ello, se decidió estimar esta probabilidad en función de la frecuencia con la que los validadores son slasheados en la beacon chain.

Con el fin de llevar a cabo una estimación precisa de esta frecuencia, es necesario tener un conocimiento detallado de la cantidad de validadores a lo largo del tiempo y de cómo ésta ha variado. Este aspecto es clave, ya que la variación en el número de validadores activos influye directamente en la probabilidad de que uno o más validadores sean slasheados en cualquier período de tiempo dado. A medida que el número de validadores crece, la probabilidad de que un evento de slashing ocurra también puede variar, afectando el cálculo de riesgos y la previsión de posibles pérdidas en la red.

Se realizó un análisis estadístico de los validadores slasheados en la red Ethereum utilizando un conjunto de datos históricos. En total, se registraron 1,131 días de actividad de slashing, con una media de 0.36 validadores slasheados por día y una desviación estándar de 3.89 validadores. Esto sugiere que, en general, los eventos de slashing son poco frecuentes y, cuando ocurren, suelen involucrar a un pequeño número de validadores.

El valor máximo de validadores slasheados en un solo día fue de 99, lo que representa un evento anómalo comparado con la mediana y los cuartiles, que se mantuvieron en cero, indicando que en el 75% de los días no se reportaron slasheos. Estos datos subrayan la naturaleza esporádica de los eventos de slashing en la red.

Justificación del cálculo de frecuencia

El cálculo de la frecuencia de slashing se realizó sobre una base diaria, debido a que este enfoque facilita la agregación y el análisis de los datos a lo largo del tiempo. Aunque los slasheos en Ethereum técnicamente ocurren durante épocas (epochs), que son intervalos de tiempo más cortos que los días (aproximadamente 6.4 minutos), trabajar a nivel diario simplifica los cálculos y permite una representación más manejable y comprensible de los eventos de slashing a lo largo del tiempo.

Los cálculos se realizan típicamente sobre la base de epochs y validadores activos. La simulación toma como referencia los períodos de tiempo en los que los validadores pueden estar inactivos o ser penalizados, considerando datos acumulados de múltiples epochs. En el caso de las penalizaciones por inactividad, el cálculo se basa en los epochs fuera de línea, mientras que para las pérdidas por slashing, se evalúa la cantidad de validadores sancionados.

Distribución de los eventos de Slashing

La mayoría de los días no presentan eventos de slashing (valor 0), mientras que unos pocos días presentaron cantidades mucho más altas, como el caso de los 99 validadores en un solo día. Este comportamiento anómalo genera una distribución sesgada hacia la derecha, lo que refleja la rareza de estos eventos de gran magnitud.

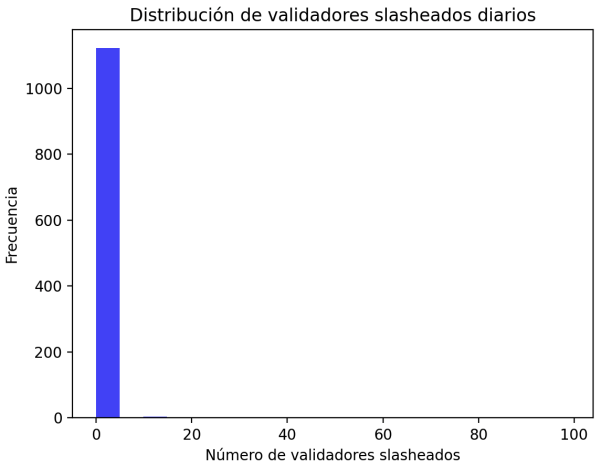


Figura 35. Distribución de los validadores slasheados.

Aunque el modelo ajustado presenta una media de 0.36 y una desviación estándar de 3.89, el ajuste no captura del todo la naturaleza dispersa y esporádica de los eventos extremos observados, lo que puede explicarse por la ocurrencia de pocos días con slasheos masivos que afectan significativamente la distribución.

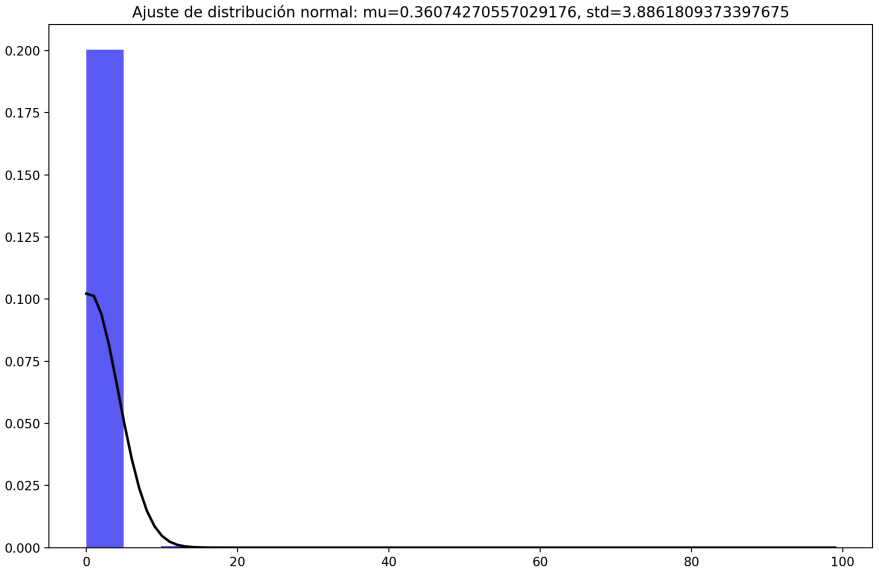


Figura 36. Ajuste de la distribución normal de los validadores slasheados.

Simulación Montecarlo para el cálculo del VaR

El Valor en Riesgo (VaR) es una medida estadística que estima la pérdida máxima esperada de una inversión o sistema en un periodo específico, dado un nivel de confianza determinado. Matemáticamente, el VaR se calcula como:

$$VaR = \mu + Z_{\alpha} * \sigma$$

Donde:

- μ: Media de la distribución (esperanza matemática).
- σ: Desviación estándar de la distribución.
- Z_{α}: Valor crítico de la distribución normal para el nivel de confianza deseado ($Z_{0.95}$=1.645 para un 95%).

Parámetros utilizados

Para esta simulación, se emplearon los siguientes parámetros:

- Media (μ): 0 validadores slasheados por día (valor observado en condiciones normales).
- Desviación estándar (σ): Calculada a partir de los datos históricos del sistema.
- Número de simulaciones: 10,000.
- Nivel de confianza: 95% ($Z_{0.95}$=1.645)

Pasos de la simulación

1. **Ajuste de la distribución**: Se asumió que el número de validadores slasheados por día sigue una distribución normal basada en datos históricos, con una media (μ) de 0 y una desviación estándar (σ).
2. **Generación de escenarios**: Se generaron 10.000 valores aleatorios siguiendo la distribución normal ajustada ($N(\mu,\sigma^2)$) para simular posibles escenarios de slashing en un día.
3. **Cálculo del VaR**:
    - Ordenamos los resultados simulados en forma ascendente.
    - Identificamos el percentil correspondiente al nivel de confianza (en este caso, el percentil 5 para un 95% de confianza).
    - El VaR obtenido fue de 0.01 validadores slasheados, indicando que en condiciones normales, el número de validadores slasheados no debería superar ese valor en el 95% de los casos.
4. **Análisis de resultados**: En el 5% de los casos extremos, los valores simulados mostraron eventos de slashing más significativos, lo que destaca la posibilidad de un impacto considerable en la red en situaciones atípicas.

12. Recomendaciones

Se decidió dividir las recomendaciones en dos: una recomendación ex ante y otra ex post.

1. Mitigación preventiva.
2. Mitigación reactiva.

12.1 Mitigación preventiva

La clave principal para mitigar riesgos es la diversificación. Por lo tanto, esta sección se dividirá en dos partes: medidas que Lido ya ha implementado y aquellas que aún no.

1. Procedimientos largos y exhaustivos para la incorporación de nuevos operadores de nodos, manteniendo su calidad y seguridad.
2. Procedimientos para la evaluación de operadores de nodos y autoevaluaciones.
3. Requisitos y procesos para mejoras en el rendimiento de los validadores.

Medidas que aún no se han implementado:

1. Asegurar que cada uno de los operadores de nodos posea menos del 1% del total de los validadores. Es importante recordar que varios operadores superan este porcentaje, con un máximo de 3.46%, lo que excede el 1% sobre el total de validadores en Ethereum.
2. Mejorar o diversificar aún más la distribución geográfica de los operadores de nodos. Actualmente, solo hay un operador de nodo en Latam, que es SenseiNode.

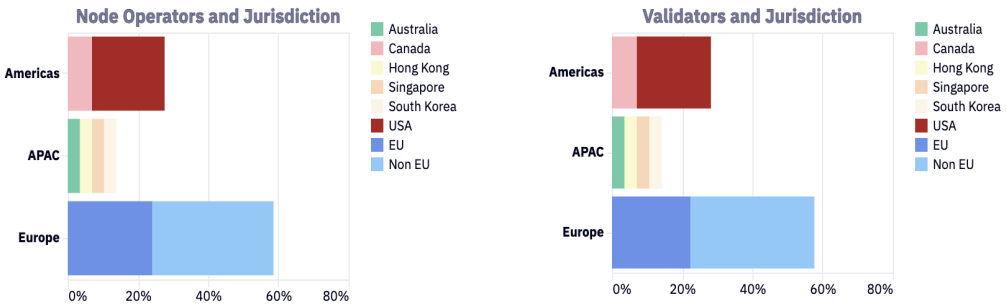


Figura 36. Distribución de nodos operadores por región.

3. Mejorar la diversificación de la distribución de la infraestructura local y de los diferentes proveedores de servicios en la nube, cabe aclarar que su implementación enfrenta limitaciones significativas que dificultan su ejecución efectiva.

4. Incrementar la diversidad de los clientes, un aspecto que ha ido mejorando a lo largo de los últimos trimestres.

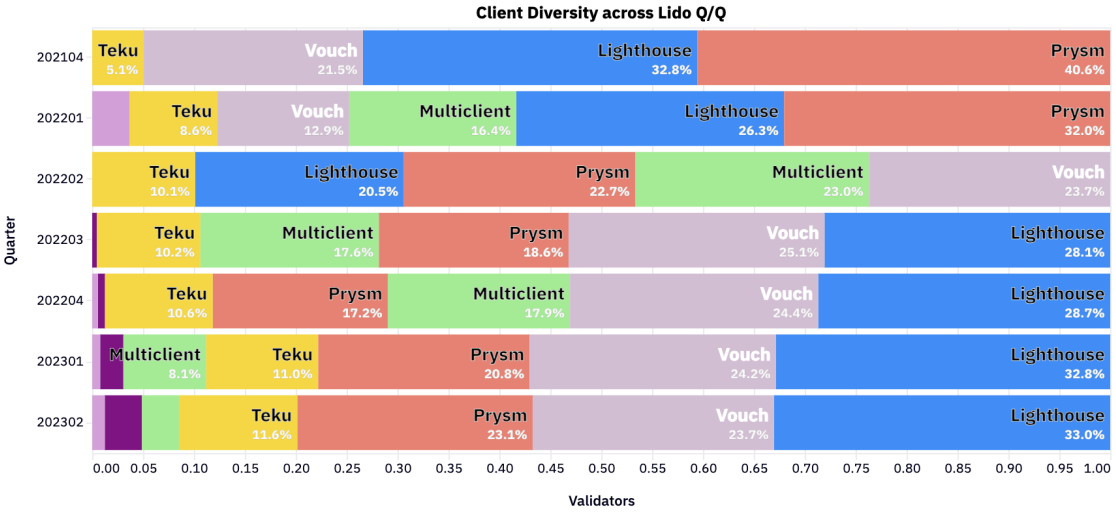


Figura 37. Distribución por tipo de cliente.

El papel de la diversidad de clientes es fundamental para la estabilidad de la red. Si más de dos tercios de los validadores dependen de un único cliente, cualquier error inherente podría desestabilizar la red y causar pérdidas significativas. La consecución de la irreversibilidad de las transacciones (finalidad) depende del consenso de más de dos tercios de los validadores. En consecuencia, un cliente predominante que experimente un error podría generar una bifurcación de la cadena principal, lo que resultaría en penalizaciones severas para los validadores respectivos, potencialmente afectando la totalidad de los 32 ETH.

12.2 Mitigación reactiva

La mitigación reactiva desempeña un papel clave en la estrategia de Lido, al proporcionar soluciones rápidas y efectivas frente a posibles perturbaciones que puedan desestabilizar el protocolo, especialmente en escenarios críticos donde la rapidez en la respuesta es esencial.

1. En el ámbito del seguro web2, la compra de contratos de reaseguro XL es una medida prudente. Estos contratos, que funcionan como un deducible, están diseñados para abordar pérdidas que superen una cantidad predeterminada, con el objetivo de contrarrestar eventos que, aunque infrecuentes, causan un daño extenso. Por ejemplo, se aconseja adquirir cobertura para incidentes que superen los 10,000 stETH. En tales casos, Lido utilizaría el fondo de seguros para cubrir los primeros 10,000 stETH, emplearía el stETH del tesoro para necesidades adicionales y activaría el contrato XL para pérdidas que excedan estos recursos.

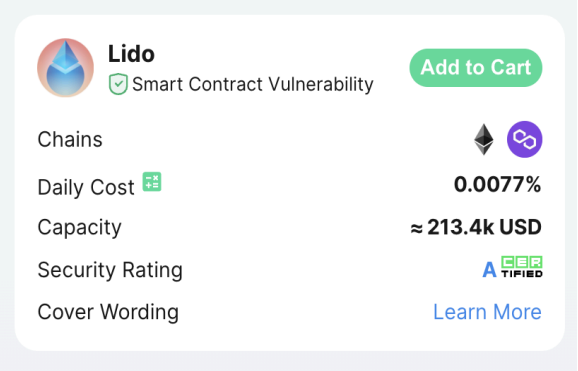


Figura 38. Imágen de la cobertura que ofrece Insurace.

2. Promover protocolos como InsurAce o Nexus Mutual para desarrollar productos dirigidos a los depositantes es crucial. Aunque existen seguros disponibles para cubrir vulnerabilidades dentro de los contratos inteligentes de Lido, estos no se extienden a validadores sancionados. Un posible obstáculo es que tales productos o coberturas sean aplicables a todos los protocolos de staking líquido y no exclusivamente a Lido. Sin embargo, un análisis exhaustivo de este aspecto está más allá del alcance de este documento (Fuente).
3. Incrementar el stETH en el Fondo de Seguros es factible aumentando la comisión actual del 10% sobre las recompensas de staking en un 1% o 2%. Esta modificación requiere un análisis más detallado para evaluar el impacto de cada incremento y medir la sensibilidad.
4. Establecer fondos de contingencia para cada validador es otro enfoque viable. Esto implicaría que cada validador asigne una parte de sus ganancias para crear un fondo similar al fondo de seguros de Lido DAO, asegurando así la compensación por pérdidas en caso de sanciones.

13. Referencias

Wang, T., Liu, J., & Liu, Y. (2020). *Security Analysis of Decentralized Finance on Blockchain.*

Schär, F. (2019). *Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets*

Qian, Z., Shinde, S., Zhou, Y., & Yin, H. (2021). *DeFi Score: A Comprehensive Framework for Evaluating Decentralized Finance Protocols*

Breitner, P., Holz, T., & Knottenbelt, W. J. (2022). *A Systematic Review of Decentralized Finance Research.*

Lutsenko, A. (2021). *DeFi Protocol Risks: An Introduction.*

Schär, F. (2021). *Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets.*

Hussain, F., Islam, M. R., & Kurniawan, Y. (2022). *A Critical Review of Decentralized Finance (DeFi).*

Warwick, K. (2020). *How to DeFi.*

Warwick, K. (2020). *How to DeFi Advanced.*

Edgington, B. (2023). *Upgrading Ethereum.*

Buterin, V. (2017, February 6). *The Meaning of Decentralization.*

Balaji, S. S. (2017, July 27). *Quantifying Decentralization.*

Chris, D. (2018, February 18). *Why Decentralization Matters.*

Rated Explorer. *Rated Labs.* https://www.rated.network/ *(accedido 17 de octubre de 2023).*

Beaconcha.In. *Bitfly gmbh.* https://beaconcha.in/ *(accedido 17 de octubre de 2023).*

Lido Blog. *Lido.* https://blog.lido.fi/ *(accedido 17 de octubre de 2023).*

Lido forum. *Lido.* https://research.lido.fi/ *(accedido 17 de octubre de 2023).*

Etherscan. *Ethereum.* https://etherscan.io/ *(accedido 17 de octubre de 2023).*

Lido Ecosystem. *Lido.* https://lido.fi/lido-ecosystem/ *(accedido 17 de octubre de 2023).*

Dune Analytics. *Dune.* https://dune.com/ *(accedido 17 de octubre de 2023).*

Llama Corp. *DeFiLlama.* https://defillama.com/ *(accedido 17 de octubre de 2023).*

Lido Finance. *(2022). Offline slashing risk analysis. GitHub.* https://github.com/lidofinance/offline-slashing-risk/tree/main *(accedido 20 de junio de 2024).*