HASHKEY Capital

ASIA CRYPTO INSIGHTS

AUG 2023

HashKey Capital

HashKey Capital is an institutional asset manager that invests exclusively in blockchain technology and digital assets. As one of the most experienced blockchain investors based in Asia, the HashKey Capital team has deep knowledge of the blockchain ecosystem in the region and has built a network connecting entrepreneurs, investors, developers, community participants and regulators.

HashKey Capital is affiliated with HashKey Group, a digital asset management and financial services institution in Asia.

Authors

Jupiter Zheng
Research Director
jupiter.zheng@hashkey.com

Henrique Centieiro
Senior Research Manager
henri.centieiro@hashkey.com

Scarlett Xiao
Senior Research Analyst
scarlett.xiao@hashkey.com

Table of Contents

HASHKEY Capital

Lagrange Labs

Friend.tech, a decentralized social platform that enables users to tokenize their social networks, has secured investment from Paradigm at an undisclosed valuation. The platform, which operates on the Base network, offers the ability to buy stakes for access to private messaging features and sell those shares at a profit (or loss).

Commentary by HashKey Capital:

Friend.tech has taken the crypto world by storm, incurring 4400 ETH (~$8.1m) in transaction volume within 24 hours of launch. Major crypto influencers have taken to the platform. Shares for the chatroom of popular influencer Cobie, for example, are now valued at >2ETH. This project is gaining traction very quickly, and even some non-Web3 native celebrities like NBA player Grayson Allen have joined the platform.

An iteration of an idea previously deployed by Bitclout, Friend.tech is one of the first SocialFi projects to achieve mainstream appeal. Friend.tech's success has demonstrated that users in the social media space are ready for major disruption, and we at HashKey are excited to see whether this is a passing jubilant moment or the beginning of a major trend.

ZetaChain

ZetaChain, a layer-1 interoperability protocol, has raised $27 million in an equity funding round from Jane Street Capital, VistaLabs, CMT Digital, GSR, Blockchain.com, and others.

Commentary by HashKey Capital:

In the rapidly changing world of blockchain technology, ZetaChain stands out as a pioneering platform that brings cross-chain interoperability to the forefront. Offering an EVM-compatible Layer 1 blockchain, ZetaChain allows for the seamless transfer of assets across multiple chains without the need for bridges or wrapped tokens. This innovative approach encompasses even non-smart contract chains like Bitcoin and Dogecoin, unlocking new possibilities in DeFi, NFTs, and beyond.

The ZetaChain ecosystem is already flourishing, hosting over 27,000 dApp contracts that span various decentralized applications like cross-chain DeFi, NFTs, and social, identity, and gaming protocols. With more than 1.7 million users engaged in its testnet and over 13 million transactions completed, ZetaChain has substantial traction. As investors, we are keen to watch ZetaChain expand its influence and capabilities, further revolutionizing blockchain interoperability.

ZTX

ZTX, a platform specializing in Web3 virtual worlds and creative content, has completed a $13 million seed funding round headed by Jump Crypto. Other significant backers in the investment include Collab+Currency, Parataxis, MZ Web3 Fund, and Everest Ventures Group, among others.

Commentary by HashKey Capital:

ZTX (ZepetoX) is a blockchain-based metaverse focusing on individuality via customized avatars, property rights, asset generation, social engagement, DeFi utilities, and community governance. Building upon the groundwork laid by ZEPETO, ZTX provides a vibrant 3D environment where creators, gamers, and communities can flourish.

Leveraging the heritage of its Web2 predecessor, Zepeto, which boasts over 400 million lifetime users, ZTX is already making waves as one of the leading metaverse platforms. Partnering with notable brands like Gucci and Starbucks, as well as cultural phenomena like the K-Pop girl group Blackpink, ZTX is perfectly poised to make a significant impact.

Section II

Blockchain Community and Market Update

Cryptocurrency project Worldcoin launches its token WLD

On July 24th, the cryptocurrency project Worldcoin, co-founded by OpenAI's founder Sam Altman and other partners, officially launched and released its token $WLD. In an open letter co-signed by Sam Altman and CEO Alex Blania, they articulated the core philosophy of Worldcoin: combining a privacy-focused digital identity with a digital currency $WLD, with the goal of building a new identity and financial system for all.

Since the beta release of Worldcoin, the number of World ID verifications has doubled in one week. In 2023, the number of World IDs created has also seen significant growth, from 1 million users at the beginning of the year to 2 million in July. Notably, the registration volume of World ID doubled in the last week. Similarly, in the first week after the release of the World App, its weekly active user count increased threefold, and the number of newly created accounts increased tenfold.

Commentary:

The development of WLD and the way it collects information have led to dissatisfaction in many countries. Currently, Germany, France, Kenya, and others have started investigating or banning the development of Worldcoin in their countries. Regardless of the final outcome of Worldcoin, this will be the first large-scale UBI (Universal Basic Income) experiment conducted for all of humanity. Previous related attempts have not attracted widespread attention. Through Worldcoin, cryptocurrency is being presented to hundreds of millions, or at least millions, of ordinary users for the first time.

HASHKEY Capital

zkSync NFT Random Airdrop Raises Fairness Doubts, Ecological Projects Massively Rug

On July 15th, zkSync released an experimental NFT project, LIBERTAS OMNIBUS, and announced that it would randomly airdrop to 10,000 early mainnet users, but only 5.5% of the addresses were eligible. However, some users within the community noticed that all airdropped addresses began with 0x0, questioning the randomness of the airdrop.

zkSync responded, stating that their use of the description "random" was inappropriate, and they plan to restart the issuance of NFTs after the EthCC conference in Paris. However, data shows that the community reaction to this has not been positive. Since July 15th, the growth rate of zkSync addresses has slipped from 19.2% to 8.8%, and its locked value has also dropped by 13.9%, leaving only $160 million. Issues have arisen in multiple projects within the zkSync ecosystem. These include an attack on the leading lending protocol EraLend, which led to a loss of $3.4 million, affecting its largest DEX in the ecosystem, SyncSwap.

Voices within the community point out that such extensive project problems are not common in coin issuance expectations. As part of the ecosystem, these projects should have close ties with zkSync, so some suspect that these problem projects may have obtained certain insider information in advance.

Commentary:

For zkSync and other cryptocurrency projects, while the airdrop strategy can quickly raise project awareness and attract a large number of users, this distribution strategy is not enough to ensure long-term user retention and loyalty. Real user loyalty comes from the construction of the project's ecosystem and its utility. If it relies solely on coin issuance expectations and airdrops, without real value creation, the halo of zkSync could fade quickly once user expectations are frustrated, and trust is broken.

HASHKEY Capital

Programming Language Vyper Vulnerability Triggers Curve Serial Attack Incident

On July 31st, the smart contract programming language Vyper announced that a flaw had occurred in its re-entrancy lock feature in versions 0.2.15, 0.2.16, and 0.3.0. Malicious attackers exploited this vulnerability using re-entrancy attacks, repeatedly signing contracts leading to fund theft. Many projects were affected, including Curve Finance, which lost up to $70 million. Luckily, some funds were safeguarded by white-hat hackers and MEV bots, with hopes of recovery.

Four pools within the Curve ecosystem were attacked, including CRV/ETH, alETH/ETH, msETH/ETH, pETH/ETH, losing more than $45 million in liquidity. In addition, nearly $25 million was lost from the CRV/ETH pool. According to DefiLlama data, Curve Finance's total locked value (TVL) fell from $3.266 billion to $1.869 billion within 24 hours, a decline of 42.78%.

Meanwhile, the price of CRV tokens on centralized exchanges fell to $0.583, and the lowest on-chain price even touched $0.109. Curve founder Michael Egorov, having acquired large loans on multiple lending protocols using his CRV tokens, could face liquidation if the price of CRV continues to fall to the liquidation standard. To prevent this, Michael Egorov started selling CRV tokens to institutions and individual investors through over-the-counter (OTC) trades, having already sold over 160 million CRV at a price of $0.4.

Commentary:

This incident serves as a wake-up call for developers and auditors of smart contracts. Ensuring the security of smart contracts requires not only paying attention to code logic but also digging deep into potential risks in underlying implementations. For hackers, this opens a new research field: compiler security. The future will see more hackers and security researchers focusing on uncovering potential vulnerabilities in compilers, intensifying the battle on this front.

HASHKEY Capital

PayPal Announces Launch of PYUSD Stablecoin

On August 7th, PayPal launched the PYUSD US dollar stablecoin issued based on Paxos, making it the first major financial institution to offer payment and transfer functions based on cryptocurrency. The value of PYUSD will maintain a stable 1:1 ratio with the US dollar, with its backing including cash deposits, short-term US government bonds, and other cash equivalents.

PayPal's intention in designing PYUSD is to make it easily convertible to dollars while also being exchangeable for other digital currencies on the PayPal platform. To enhance this functionality, PayPal plans to integrate PYUSD into its payment app, Venmo, allowing users to make seamless token transactions between PayPal and Venmo. In addition, because PYUSD is based on Ethereum's ERC-20 standard, users can also transfer it to other wallets compatible with PayPal, expanding its use cases. To ensure the security and reliability of its stablecoin, PayPal will first conduct payment tests among institutional clients before launching it for general users in the United States.

Commentary:

The design of PYUSD currently outperforms most stablecoins. PYUSD and its reserve assets will be strictly regulated by the New York Department of Financial Services (NYDFS), which means that even in the event of Paxos Trust's bankruptcy, customer assets will not be used to repay Paxos's debts. By leveraging the advantages of PYUSD in on-chain payments, it is possible to rebuild Web2 world business scenarios on Web3 and bring new benefits. PYUSD may become an important tool for PayPal to build Web3 business scenarios in the future.

HASHKEY Capital

U.S. Releases July Inflation Report, CPI Lower Than Expected

On August 10th, the U.S. Department of Labor released its July inflation report, with both the overall and core CPI annual rates falling short of expectations. The data indicated that the U.S. overall CPI annual rate for July was 3.2%, lower than the expected 3.3%, but higher than the previous value of 3%, marking the first acceleration since June 2022. The U.S. core CPI annual rate for July was 4.7%, a new low since October 2021, and 0.1 percentage points lower than both the expected and previous values.

The market responded positively to the July CPI report, with futures for the three major U.S. stock indices all climbing after the data was released. The swap market showed a decreased likelihood of the Federal Reserve raising interest rates again within the year. According to CME's "Fed Watch," the likelihood of the Federal Reserve keeping interest rates unchanged at 5.25%-5.50% in September is 90.5%, while the probability of a 25 basis point hike to the 5.50%-5.75% range is 9.5%. By November, the likelihood of interest rates remaining unchanged is 74.7%, with a 23.7% chance of a cumulative increase of 25 basis points, and a 1.7% chance of a cumulative increase of 50 basis points.

Commentary:

Looking at the specifics, items including housing, car insurance, education, and entertainment all saw increases. Airline tickets, used cars and trucks, medical services, and communication prices all decreased in July. Housing inflation was the largest contributor to CPI. The month-on-month increase of 0.2% is viewed as moderate inflation, which is what Fed officials would like to see. Future U.S. inflation is expected to continue to decrease, and weak demand will accelerate this decrease in the coming months.

HASHKEY Capital

SEC Delays Decision on BTC ETF, ETH Futures ETF May Launch This Year

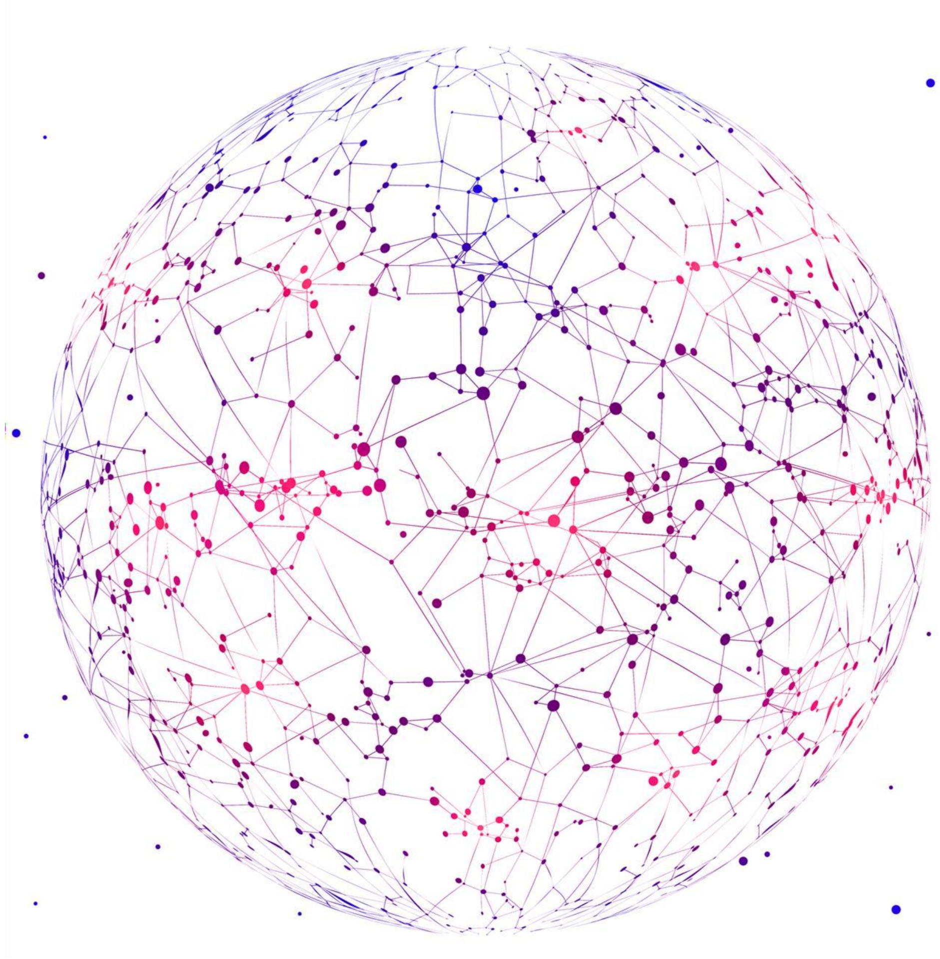
August 13th was the second deadline for the Bitcoin spot ETF application jointly submitted by 21 Shares & ARK. The SEC has yet to make a final decision, while multiple ETF applications from BlackRock, Bitwise, and others are awaiting initial statements from the SEC in early September. The market, in general expects the SEC to respond uniformly to these ETF applications in January 2024. Meanwhile, insiders have reported that the SEC is prepared to allow the first Ethereum-based futures ETF. Given that the Bitcoin futures ETF has been approved for over a year, the likelihood of this news being true is relatively high.

Commentary:

Since BlackRock applied for the spot ETF at the end of June, the market has been continuously watching the SEC's statements, which has led to a prolonged period of sideway low-volatility in the market over the past month. Whether or not the ETF is approved will also determine if there will be incremental funds entering the crypto market in the future, thus influencing future trends. The probability of the Ethereum futures ETF is likely to have the same impact as the Bitcoin futures ETF, and it won't have a significant impact on the market. It is more of a market signal.

Section III

Listed Companies & Token



- **BIT Mining Q2 financial report: Revenue of $74.1 Million, Down 62% Year-on-Year**

  Source: https://www.prnewswire.com/news-releases/bit-mining-limited-announces-unaudited-financial-results-for-the-second-quarter-ended-june-30-2023-301904479.html

  Hut 8 Mining Q2 financial report: Produced 399 bitcoins, of which 396 bitcoins have been sold

  Source: https://www.prnewswire.com/news-releases/hut-8-reports-operating-and-financial-results-for-q2-2023-301899327.html

  Bitcoin mining company Bitfarms releases financial report: Mined a total of 1223 Bitcoins in Q2, with revenue of $35 million

  Source: https://www.globenewswire.com/news-release/2023/08/08/2720416/0/en/Bitfarms-Reports-Second-Quarter-2023-Results.html

Section IV

China Blockchain Headlines

People's Daily: Promoting Blockchain Industry Development Through National Standardization

The People's Daily (July 28, 2023, Page 05) published an article announcing the introduction of the first national standard in the field of blockchain technology. The "Blockchain and Distributed Ledger Technology Reference Architecture" was recently released, standardizing blockchain systems' functional architecture and core elements. It provides a reference guide for the industry to unify the understanding of blockchain concepts, construct complete blockchain systems, and choose blockchain services. This standard is a basic and universal standard guiding blockchain technology's application and industrial development in China and has already been applied in hundreds of typical blockchain enterprises.

Establishing standards is one of the signs of an industry's maturity. The application of blockchain technology has expanded constantly in finance, energy, supply chain, judiciary, and other fields in just a few years since its emergence. Previously, China had issued dozens of industry and group standards for the blockchain sector, but the effect of implementing these standards was not ideal, and there was a lack of a "common language" among different blockchain systems. The development of national standards helps to achieve secure and reliable information interaction between different blockchain systems, build an open-source ecosystem, and accelerate the creation of a complete blockchain industry chain.

Chengdu Provides Special Subsidies to the Blockchain Industry

The Chengdu Economic and Information Bureau and the New Economy Commission recently announced the release of the "Implementation Rules for Special Policies for the Construction of the National Blockchain Innovation Application Comprehensive Pilot in Chengdu" and the "Implementation Rules for Special Policies to Promote the Development of the Big Data Industry in Chengdu (Revised)". Both of these policies aim to support the development of relevant industries.

According to the new rules, entities that establish blockchain technology evaluation institutions can receive a one-time subsidy of up to 2 million RMB. Enterprises that independently invest in the construction of data service platforms can receive a subsidy of up to 3 million RMB.

These measures highlight the city's commitment to fostering the growth of the blockchain and big data industries and could serve to attract more businesses in these fields to establish operations in Chengdu.

Section IV

China Blockchain Headlines

Zhejiang: Accelerating the Construction of the Metaverse Future Industry, Encouraging Significant Iconic Achievements in Fields such as Blockchain

Zhejiang held a provincial conference on the high-quality development of the platform economy, with representatives from 100 platform companies, including Alibaba and NetEase. This is the first provincial conference in the country with the platform economy as the theme. The conference issued the "Implementation Opinions on Promoting the High-quality Development of the Platform Economy," the first such opinions in the country.

The "Opinions" encourage platform companies to achieve a series of key achievements in fields such as blockchain and promote the construction of computational infrastructure. Platform companies are encouraged to use innovative technologies such as blockchain to create diverse application scenarios for the future.

The province aims to accelerate the construction of new advantages in the metaverse future industry, support diversified entities to build comprehensive experimental platforms for the metaverse, strengthen the application of the metaverse in multiple scenarios, and promote the industrialization, scale, and internationalization of the metaverse industry chain in all aspects.
Moreover, platform companies are encouraged to participate in the pilot program of the digital RMB.

HASHKEY Capital

The LSD Contenders for DeFi's Next Big Thing

In this Asia Crypto Insights, we cover 11 largest LSD protocols by TVL – Total Value Locked.

We have covered the LSD landscape in the previous Asia Crypto Insights. For the full report, please check this link.

The LSD space has been adding billions of dollars in TVL and it's likely to continue growing over the coming years, potentially becoming a trillion-dollar industry. In this section, we break down these LSD protocols, giving the community an in-depth understanding of all these DeFi protocols.

	Lido	Coinbase	Rocket Pool	Frax	StakeWise	Ankr	Stader	Ether.fi	Stafi	Swell	NodeDAO	Stakehouse
LSD token	stETH	cbETH	rETH	frxETH + sfrxETH	sETH2 + rETH2	ankrETH	ETHx	eETH	rETH	swETH	nETH	dETH
Token Mechanism	Rebasing token	Reward bearing token	Reward bearing token	Base token + reward bearing token	Base token + reward bearing token	Reward bearing token	Reward bearing token	Reward bearing token	Reward bearing token	Reward bearing token	Reward bearing token	Reward bearing token
Commission	10%	25%	15%	10%	10%	10%	10%	0% (for now)	5%	0% - 5%	10%	Depends
Commission Distribution	Validators: 5% Lido DAO: 5%	Coinbase: 25%	Pool validators: 15%	Frax treasury: 8% Fund: 2%	Stakewise DAO and node vaults	Nodes and project treasury	5% to the DAO, 5% to nodes	N/A	3.5% to FIS token holders, 1% to treasury, 0.5% stafi team	N/A	7% distributed to node operators and 3% to NodeDAO	Depends on governance
# node operators	29	1	2 800	1	3	3	N/A	Multiple	1	N/A	N/A	N/A
Min. staking for validators	N/A (permissioned)	N/A (permissioned)	8	N/A	N/A	N/A	4	Permissioned ATM	12 ETH	N/A	1.1 ETH	Depending on governance.
Governance token	LDO	N/A	RPL	FXS	SWISE	ANKR	SD	N/A	FIS	N/A	N/A	N/A
Token mcap	$1 556 mil	N/A	$783 mil	$405 mil	$18 mil	$165 mil	$20 mil	N/A	$16 mil	N/A	N/A	N/A
TVL/mcap	0.12	N/A	0.46	0.53	0.11	1.23	0.25	N/A	0.64	N/A	N/A	N/A
FDV	$1 769 mil	N/A	$783 mil	$558 mil	$66 mil	$165 mil	$118 mil	N/A	$31 mil	N/A	N/A	N/A
% circ. supply	88%	N/A	100%	72%	27%	100%	17%	N/A	53%	N/A	N/A	N/A

*June 2023

Lido

Summary: Lido is the leading LSD space in terms of TVL with over $14 billion under management. It was launched in Dec. 2020, right after the Ethereum Beacon chain went live and saw a meteoric rise, becoming the most popular LSD protocol.

Although also providing staking LSDs on Solana, Moonbeam, Mooriver, Polkadot, Kusama and Polygon, Lido is most well known for having around 34% of all staked ETH and 75% of the LSD market share on Ethereum. Lido has received some criticism for being a centralization point, but the protocol has been moving towards decentralization, making those concerns less legit. Although the community talks a lot about the risks of Lido's centralization, Lido's TVL grew 30% in the 3 months after the Shanghai upgrade, showing that general users are more concerned about convenience than decentralization

Token use and type and tokenomics: Users can stake any amount of ETH and receive 1:1 stETH token. Lido's stETH token is a rebase token, meaning that the user's balance of stETH will automatically update daily to reflect the rewards. Users need to consider that most DeFi smart contracts will not compute token rebasing and the user might lose those rewards unknowingly. For this reason, it's worth exploring pools with wstETH token instead, as the wrapped version can always rebase. Users can wrap stETH from the Lido app.

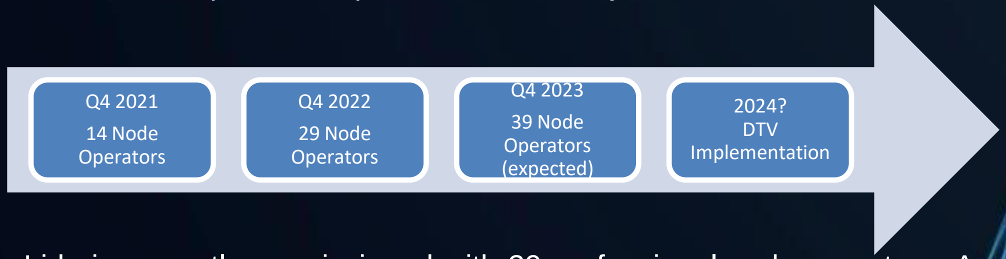
The LDO token is the governance token, meaning that it can be used by users voting in Lido's governance process. At the time of the writing, 99% of the supply is unlocked and circulating.

Commission/fee: Lido charges a 10% fee on the staking rewards. Over the last year, Lido accumulated $735 million in fees, and the DAO treasury seats at $260 million as of August 2023.

Lido

Node operators: Lido's node operators are onboarded in a permissioned/curated manner. A strict onboarding process has been needed as Lido needs to ensure the node operator infrastructure robustness/resilience, performance and ethos alignment. As of August 2023, Lido has 29 node operators, but the DAO is onboarding more node operators.

Lido has been testing during Q1 2023 DVT – Distributed Validator Technology – that will bring more decentralization to Lido's node operators, allowing anyone to participate as a node. This is an important step to further diversify and decentralize the Lido node infra.

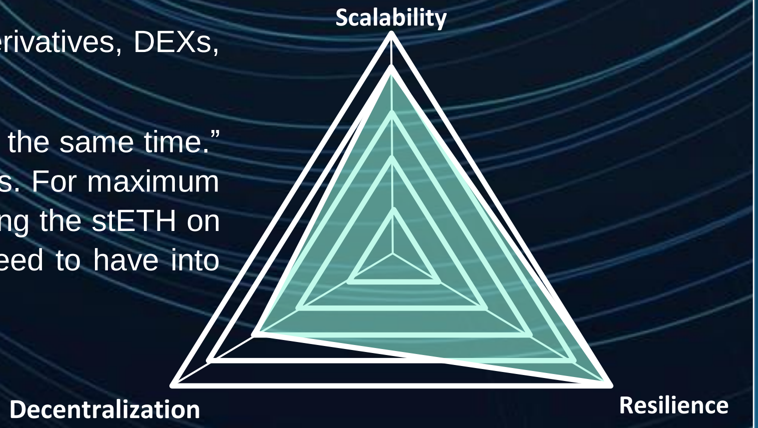


Permissioned/less: Lido is currently permissioned with 29 professional node operators. As mentioned, Lido is moving to a more permissionless model by integrating DVT and staking routers. Lido has piloted with both SSV and Obol.

Slashing protections: both stakers and node operators are subject to slashing risks. However, the Lido DAO does have a slashing insurance fund that can be activated as a self-insurance. In April 2023, the Lido DAO voted for using the insurance fund to cover the slashing of the RockLogic slashing incident. As per April 2023, the insurance fund has approx.. $11.11 million.

DeFi and LSDfi compatibility: stETH is currently accepted in 122 different DeFi protocols, from lending protocols, derivatives, DEXs, asset management and others, giving it high usability, liquidity, and capital efficiency.

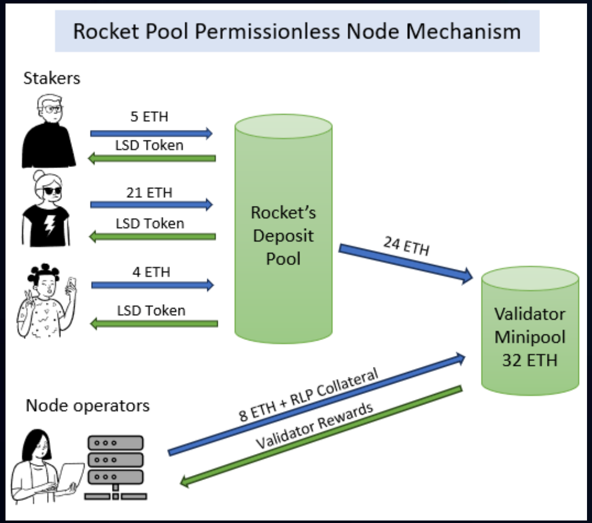
Capital efficiency: Lido stETH offers a great level of capital efficiency and the users can "have their cake and eat it at the same time." Users that deposit ETH, receive a highly liquid token – stETH – that, as we saw, is compatible with 122 DeFi protocols. For maximum capital efficiency, some users use looping strategies that involve for example staking ETH on Lido for, stETH, depositing the stETH on Alchemix to get an ETH loan and stake this ETH back on Lido. This can be looped a number of times, but users need to have into account smart contract risks.



Rocket Pool

Summary: Rocket Pool is the OG LSD. Founded in 2016, its main goal is lowering the ETH staking technical and financial barriers while improving validator decentralization. Rocket allows users to stake any amount starting from 0.01 ETH and receive liquid rETH tokens. Rocket Pool is the biggest permissionless LSD protocol, allowing anyone to join as a validating node. While the minimum to be a validator was 16 ETH until the Atlas upgrade on April 2023, which reduces the node requirement to 8 ETH.

By running two 8 ETH minipools instead of one 16-ETH minipool, the capital requirement for operating a validator is significantly reduced, resulting in higher returns for both the node operator and the rETH stakers.



Rocket pool is one of the protocols that has grown the fastest since the Chapella upgrade, with a 94% growth 2 months after the upgrade.

Token use and type: rETH is a reward-bearing token (i.e. a cToken), that automatically accrues staking rewards based on the Rocket Pool staking rewards. rETH can be traded for ETH at any time. There are approx.. 18 500 rETH token holders. Being a non-rebasing token, its integration with DeFi protocols is straightforward.

HASHKEY Capital

Rocket Pool

Commission/fee: Validators can either stake 16 ETH or 8 ETH. The first pays 20% from the generated yield, while the second pays 14%. This incentivizes node operators that have 16 ETH or more to create 2 “8 ETH mini pools” and run 2 nodes instead of 1.

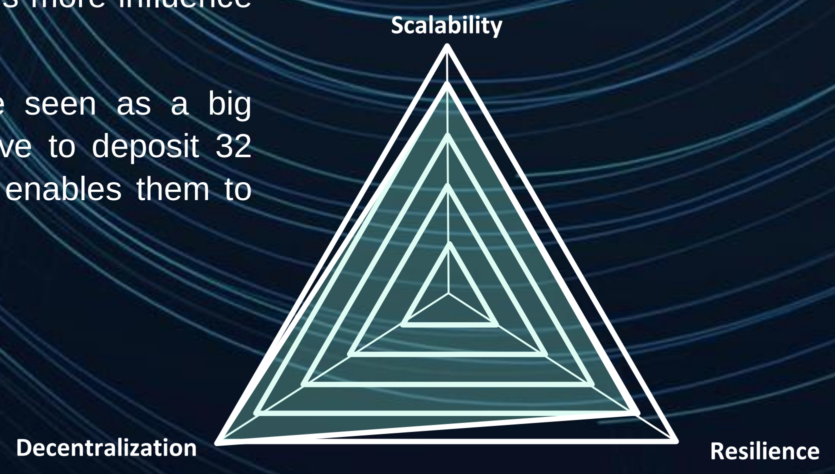
Node operators: To participate, operators need to provide a RPL collateral with a minimum of 10% of the borrowed amount of ETH and a maximum of 150% of the bonded amount of ETH. This drives the demand for RPL token and creates another utility for the token: node collateral. On the other hand, adds an entry barrier to validators.

Node Operators receive 3 types of rewards: staking rewards (100% of their staking rewards), commissions (15% of the yield generated by rETH depositors), and RLP rewards that come from locking RLP as collateral.

Decentralization: Rocket Pool is permissionless and trustless, meaning that anyone can join as a node operator. Rocket Pool has over 3100 node operators that manage a total of 24 600 validator nodes at the time of the writing, making it one of the most decentralized LSD option.

Rocket Pool governance is distributed across 2 DAOs: Oracle DAO (oDAO) and the Protocol DAO (pDAO) and over 700 members participate in the voting. The governance model includes a “power scoring” that gives more influence to smaller token holders. Similarly to quadratic voting, this helps balance the power across voters.

Capital efficiency and DeFi compatibility: requiring the node operators only 8 ETH can be seen as a big accomplishment from the capital efficiency perspective (considering that a solo staker would have to deposit 32 ETH). Moreover, the node operators can benefit greatly from the low staking requirement, which enables them to accumulate interest if they choose to do so.



Frax Ether

Summary: The issuer of the FRAX stablecoin is also climbing up the ranks of the top LSD staking platforms with its product Staked Frax Ether (sfrxETH). FRAX staked ETH TVL rose by 72% within the first 2 months after the Chapella upgrade, being in this aspect best performer just behind Rocket Pool.

Frax encompasses a number of products that evolved primarily from the FRAX stablecoin: an AMM, Fraxlend, and Ferry (a cross-chain bridge).

Being an OG in the decentralized stablecoin ecosystem, Frax developed a significant ecosystem around its stablecoin FRAX that now expands its use cases to the LSD space.

Frax offers one of the highest LSD yields and facilitates the staking process to users who want to access ETH liquid staking. In recent months it gained enough traction to claim over 2.4% of the market share, making it 4 largest LSD protocol.

Token use and type: There are 2 tokens: frxETH, which acts as a stablecoin soft-pegged to ETH, and sfrxETH, the staked token that accrues yield. The rewards earned by the validators are distributed to the sfrxETH holders. Similarly to rETH, sfrxETH value goes up over time. The token can be used in different DeFi protocols, including Fraxlend.

sfrxETH and frxETH are interchangeable. To stake ETH on Frax, users need first to mint frxETH and then stake it to receive sfrxETH. sfrxETH is an ERC-4626 vault token that represents a fractionalized ownership of the staking yield-bearing vault.

Commission/fee: Frax charges 10% commission. This commission is divided between 2% to a slashing insurance fund and 8% distributed to Frax shareholders (FXS).

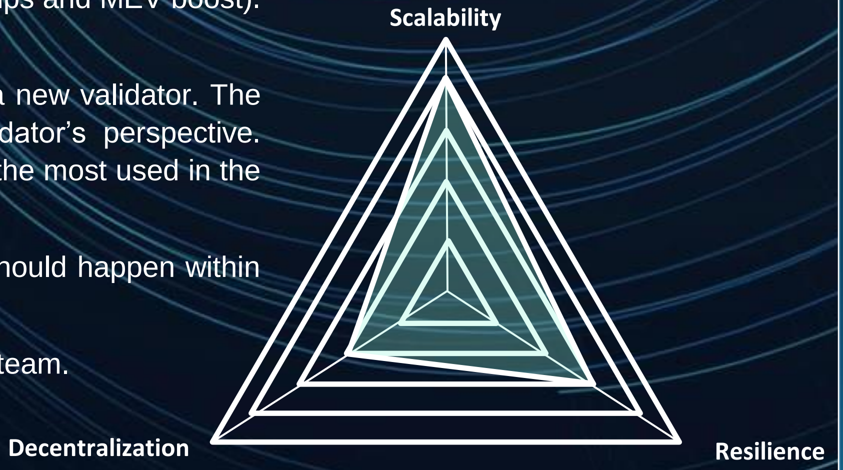
Rewards: Having a 10% fee, sfrxETH ends up paying one of the best yields among its LSD peers (from staking yields, tips and MEV boost). Additionally, frxETH and sfrxETH can also earn additional boosted rewards from Curve pools.

Node operators: Whenever a deposit pushes the minter balance over 32 ETH, the contract automatically spins up a new validator. The Frax core team is the main node operator of the validating nodes, making it quite decentralized from the validator's perspective. Additionally, all Frax validators (over 6000), are running only 2 clients: Lighthouse and Prysm. Being these two clients the most used in the market, Frax doesn't add much to client diversity.

Frax has plans to move to a more decentralized option similar to Rocketpool. This update will come with V2, which should happen within Q3 2023.

Decentralization: at the time of writing the report, Frax is the only node operator, where the nodes are operated by the team.

DeFi and LSDfi compatibility: sfrxETH is compatible with 23 different DeFi protocols. 11.5



HASHKEY Capital

Ankr

Summary: Ankr is an infrastructure protocol with an LSD offering. In a nutshell, Ankr is a suite of decentralized products and infrastructure marketplace that covers a number of different products for Web3 and DeFi. Ankr's main product is to connect a decentralized network of nodes with Web3 developers in a decentralized marketplace with RPC services for 37 different chains. However, on the LSD side, Ankr offers LSDs for Ethereum, Polygon, BNB, Fantom, Avalanche, Polkadot and Kusama.

Users that stake ETH receive ankrETH which is a rewards bearing token that accrues rewards by increasing in value in relation to ETH.

Ankr offers ample APIs and SDKs that allow developers to easily integrate with Ankr's liquid staking and crowdloan services.

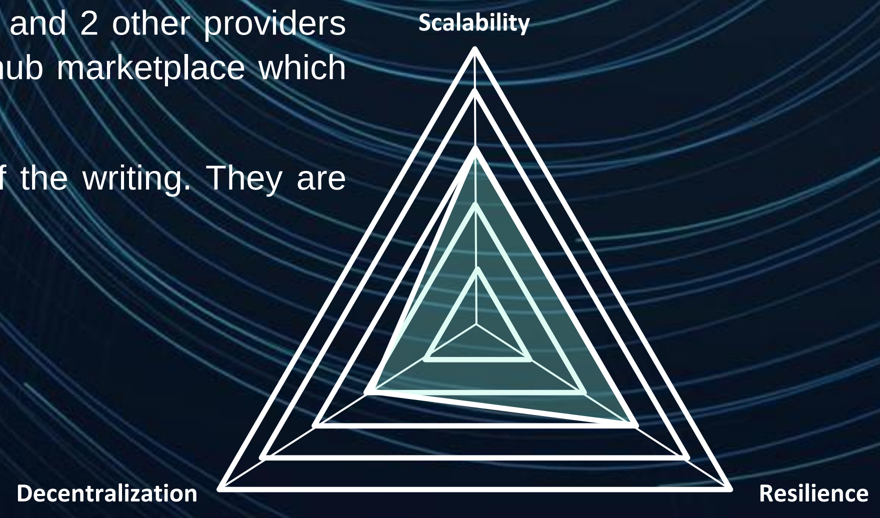
Token use and type: ankrETH is a reward-bearing token that accrues value daily. ankrETH holders can swap the LSD token to ETH on a DEX or unstake/redeem 1:1. Unstaking takes 4 days but users can opt for a flash unstake that allows for instant release of funds with a 5% commission.

Commission/fee: Ankr takes a 10% fee from the staking rewards. The fees are distributed across node providers, security audits and other needs to support project.

Node operators: Ankr staking is currently distributed across 3 node operators, being Ankr and 2 other providers that are only known to the team. The Ankr team plans to implement DVT and a validator hub marketplace which will bring more decentralization with the future upgrade. This might include SSV and Obol.

Decentralization: as previously mentioned, there are only 3 node operators at the time of the writing. They are concentrated on 2 clients: Lighthouse and Prysm.

DeFi and LSDfi compatibility: Ankr is compatible with only 3 DeFi protocols.



Stakewise

Summary: StakeWise has been consistently rising in terms of TVL, although its market share is still approx.. 1%. The StakeWise non-custodial pool allows users to gather resources the ETH 32 that are necessary for node operators to stake on behalf of the pool depositors. Node operators can join a permissionless manner with StakeWise V3. There's no staking minimum for users.

The StakeWise pool allows users to deposit ETH in exchange for sETH2, the LSD token that represents ownership of the staking pool.

Token use and type: the rewards are distributed to the users according to their share in the pool. StakeWise has two different tokens: sETH2, which represents staking ETH and rETH2 which represents the rewards. Both can be redeemed 1:1 and both are ERC20 tokens.

Unlike reward-bearing tokens, for users to compound their earnings, they need to redeem the rewards and re-stake them.

StakeWise tokenomics are likely to change once V3 is implemented.

Commission/fee: StakeWise charges a 10% fee on the rewards.

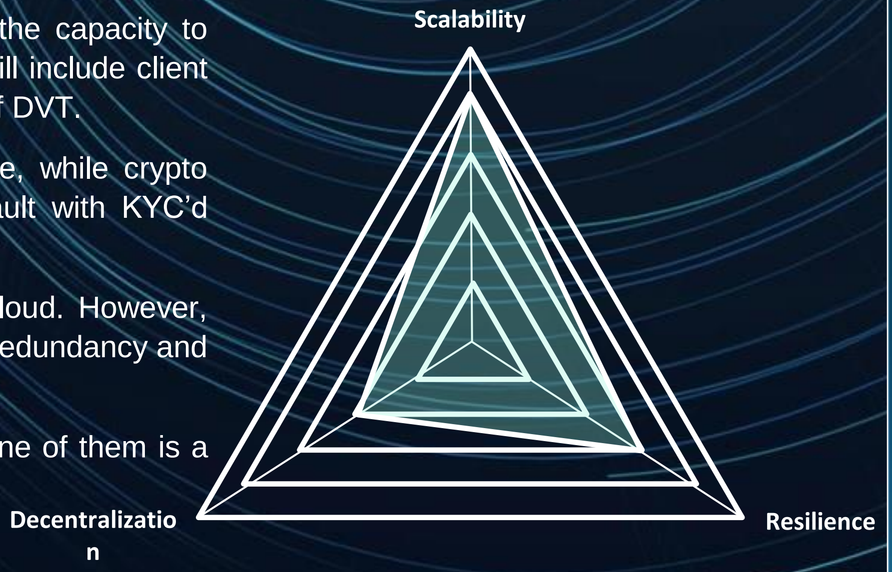
Node operators: StakeWise has been operating in a centralized model where it operates the validators in a cloud provider. The cloud infrastructure used can scale up automatically if necessary, taking advantage of auto-scalling capabilities provided by the different cloud providers. However, V3 will introduce the possibility for validator nodes to join StakeWise in a permissionless manner.

On V3, node operators will be distributed across different vaults/mini-pools and users/stakers will have the capacity to choose from a vault marketplace which vault they would like to use based on the vault score. This score will include client diversification, node performance, collateral, slashing insurance metrics, geographical diversity, and usage of DVT.

The creation of private vaults allows stakers to choose a vault that better fits their profile. For example, while crypto community users can opt for a permissionless vault, institutional users might want to use a private vault with KYC'd validators and OFAC enforcement.

Decentralization: at the time of the writing, StakeWise is still mostly centralized and operated on the cloud. However, StakeWise V3 will allow validating nodes to join in a permissionless manner and adopt DVT for added node redundancy and decentralization. V3 will introduce DVT technologies like SSV and Obol.

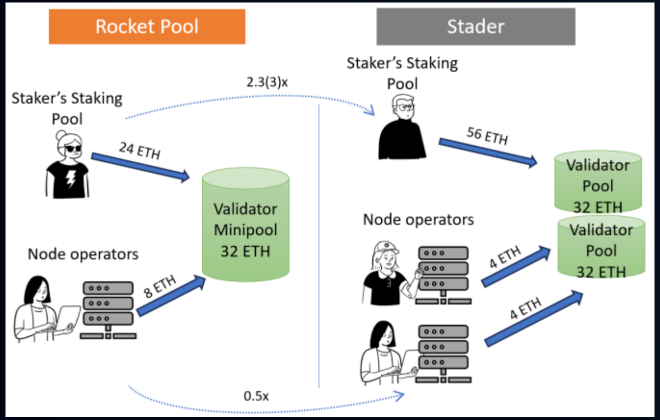
DeFi and LSDfi compatibility: sETH2 is, at the time of the writing, compatible with 10 DeFi protocols. None of them is a lending protocol.

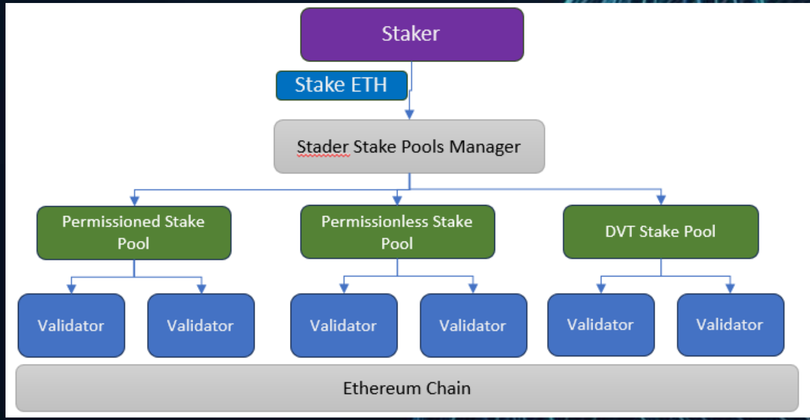


Stader

Summary: Stader is a multichain LSD protocol that started with Terra but expanded to other chains after the Terra/Luna collapse. Although compatible with different chains, Ethereum is likely to become the majority of Stader's TVL in the future. Stader offers a convenient way to stake ETH and maximize staking returns.

Stader launched recently the ETH staking solution called ETHx which promotes decentralization and scalability of liquid staking solutions by having multi pool and modular applications. Validator operators are able to stake ETH 4 only to run a validator in the Stader permissionless pools, which is substantially lower than the ETH 32 required to be a solo staker. This is great for node operator capital efficiency and it's in line with their vision of allowing one validator node in every home. Individual validators get additional fee/commission from the 28 ETH staked by users.

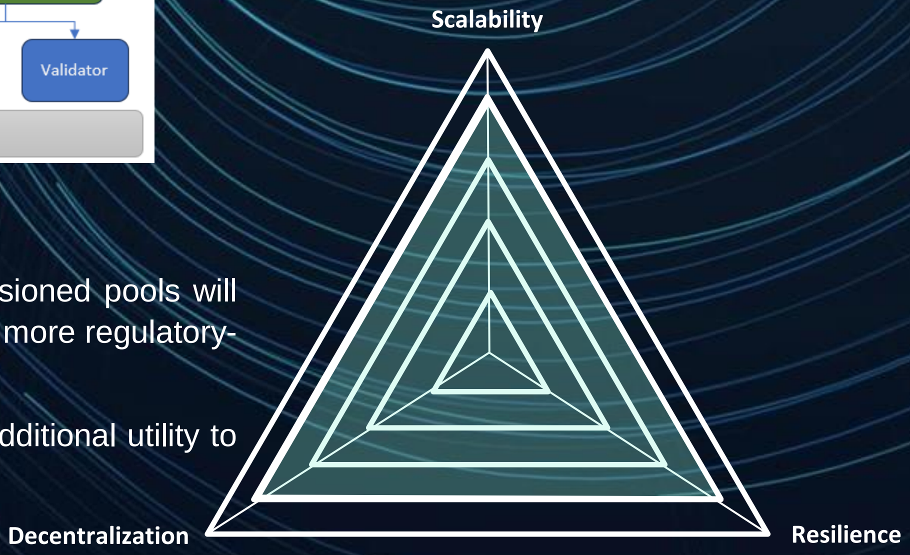




Stader pushes validator capital efficiency one step further.

Stader will be using SSV's DVT infrastructure for improved resiliency and decentralization. Permissioned pools will also be created for high-performance validator operators and institutions to be able to participate in a more regulatory-compliant manner (e.g. OFAC).

Stader takes 10% of the staking rewards, where 5% are put towards the StaderDAO, which gives additional utility to the Stader token. In addition, node operators need to bond 0.4 ETH worth of SD tokens per validator.



HASHKEY Capital

Ether.fi

Summary: Almost all LSD protocols claim to be decentralized but Ether.fi seems to be on the right path for a fully decentralized staking network where the stakers keep control of their keys. Ether.fi already attracted approx. $25 million in TVL to its incentivized early adopters program. Is Ether.fi the coolest project in the LSD space? Well, at least Ether.fi saw a 69% growth in the 2 months post-Chapella.

Ether.fi uses NFTs in a clever way. For every 32 ETH staked, 2 NFTs are minted: a T-NFT and a B-NFT. The T-NFT is transferable and represents a 30 ETH interest on the validator. The B-NFT or Bonded NFT represents the remaining 2 ETH and can be used as a slashing insurance NFT.

Ether.fi is running their EAP – Early Adopter Program – allowing users to deposit ETH, wstETH, rETH, sfrxETH, cbETH to earn bonus points that will give them access to boosted rewards. The goal is to bootstrap the initial liquidity.

Token use and type: Ether.fi's LSD token eETH is a reward-bearing token.

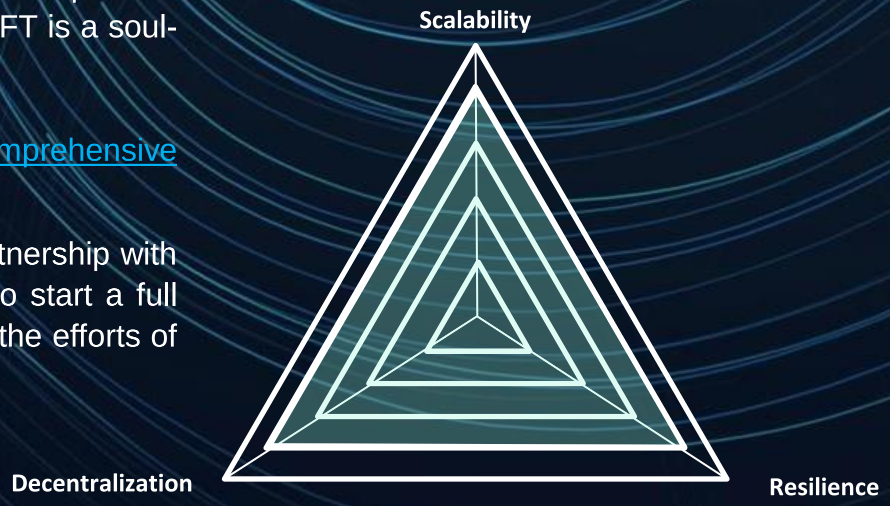
Commission: 0% during the EAP phase. The commission will increase after the EAP phase.

Private key management: Ether.fi's delegated staking allows users to stake multiples of 32 ETH and control their keys - similarly to Staking as a Service provider. The main difference, in this case, is that everything is done in a decentralized and permissionless manner.

In this case, the staker keeps control of the private keys and receives the 2 NFTs mentioned above that represent its stake. The T-NFT can be transferred/liquidated (which brings liquidity to the staker), while the B-NFT is a soul-bonded token. The node operators will also keep their own node operator keys.

Node operators: node operators can join in a permissionless manner. Ether.fi offers comprehensive documentation and a user-friendly UI to help new operators join with new validating nodes.

At the time of the writing, Ether.fi is running a promotion called "Operation Solo Staker" where in partnership with Obol, dappnode and Avado, they offer the users the hardware (node), and the capital necessary to start a full node. In exchange, node operators need to commit to operating the node for 3 years. This is part of the efforts of the protocol to keep the validator network decentralized since its very start.



Stafi

Summary: Stafi provides LSDs for multiple chains, including Ethereum, Polkadot, Kusama, Polygon, BNB, Solana, Cosmos, IrisNet, Chihuahua, and Carbon.

Stafi is a decentralized protocol built on Substrate, and it's part of the Polkadot ecosystem. Ethereum stakers are able to stake any amount starting from 0.01 ETH. Stafi connects stakers with validator nodes, giving priority to "well-performing" nodes.

Token use and type: Stafi's rTokens (rETH) are reward-bearing tokens. Its exchange rate is always positively correlated to the staking income. Once users stake ETH, Stafi automatically mints new rETH for the user (do not confuse it with RocketPool's rETH). 1:1 unstake is already available. rETH is also available for swap in multiple exchanges.

Commission/fee: Stafi offers one of the lowest commission fees in the LSD space: 5%. The revenue from the fees is distributed across the FIS token holders (70%), Stafi treasury (20%), and Stafi team (10%).

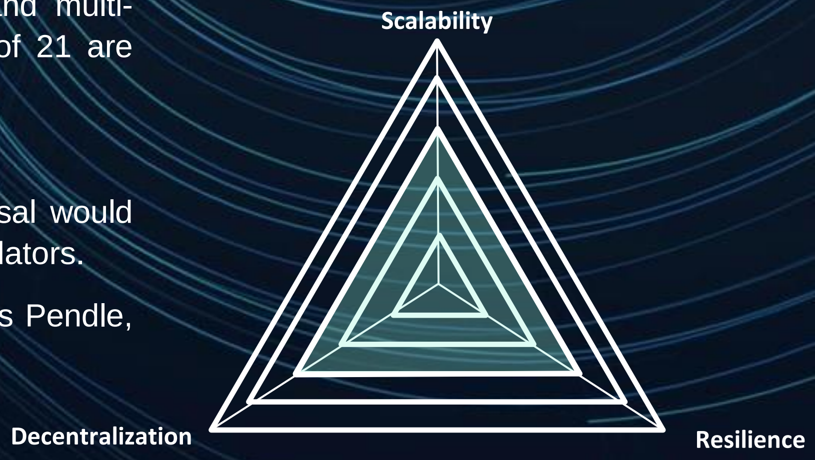
Node operators: Stafi has committed to decentralization since day one and Stafi run their own validating nodes. Stafi offers two options for validators – permissionless solo validators and permissioned trusted validators. The permissionless option allows anyone to join as a validating node by depositing 12 ETH to register the node. Stafi rETH pool will allocate the remaining 20 ETH to the validator. The "trusted validator" option allows the node operators to join with zero ETH but they are KYC'd and sign legal agreements.

Private key management: the staking contract is managed using MPC – Multi-Party Computing and multi-signature. 21 fragments of the staking contract are distributed across unspecified validators. 16 out of 21 are necessary to recover the private key. Additionally, the nodes that have the keys are rotated every 6 hours.

Decentralization: According to rated, the majority of the Stafi validators use one single client – Prysm.

Stafi governance is currently discussing the implementation of the DVT infrastructure SSV. This proposal would improve the decentralization and security of the protocol, as well as reducing the entry barrier for new validators.

DeFi and LSDfi compatibility: rETH is compatible with close to 10 DeFi protocols, being the main ones Pendle, Uniswap, Balancer, Curve, Aura, Convex, and Camelot.



Swell

Summary: Swell is a non-custodial ETH LSD protocol. It went live in Q2 2023 and it has been running an early adopter program to bootstrap liquidity. As of August 2023, it has attracted close to $80 million in liquidity. There's no minimum staking amount and Swell aims to be a fully decentralized and permissionless staking network using DVT technology. However, it started with a permissioned validator set where node operators are vetted.

Token use and type: Swell's swETH token is a reward bearing token. Similarly to other LSD protocols, the rewards accrued include rewards/penalties from the Consensus Layer, MEV and tips from the Execution Layer. The amount of swETH doesn't change but its value changes. The SWELL governance token is not available yet but it will be used for the DAO community, governance and to incentivize growth.

Commission: as of the time of the report, Swell has been running a 0% fee promotion. Once the promotion is finished, a 5% commission will be applied. This commission will be necessary to attract new node operators.

DeFi and LSDfi compatibility: swETH is compatible with 9 DeFi protocols.

HASHKEY Capital

NodeDAO

Summary: NodeDAO is one of the most recent LSD protocols in the space. Since the start, NodeDAO strived to be a decentralized validator system, although it started with a "trusted validator set."

NodeDAO uses HashKing (an aggregator) to manage the node operators from different Web3 infrastructure providers – ChainUp Cloud and XHash and more. The protocol is also in the process of integrating with SSV's DVT technology for better decentralization and any person can easily create a validator node. There are 2 options for users: nETH and vNFT. nETH is LSD similar to Lido. vNFT is non-custodial and similar to other Staking as a Service providers. Users can also become an operator and create the validator node themselves.

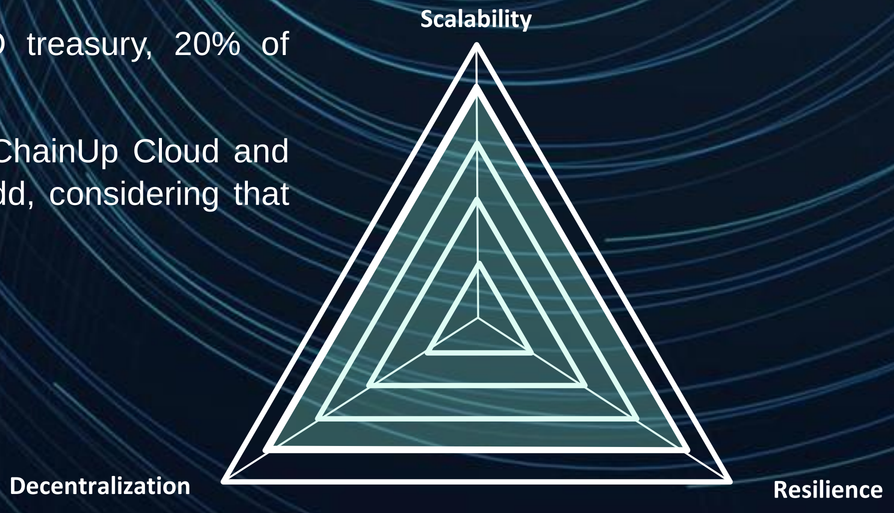
Once the user creates a node and deposits the 32 ETH, he can mint an NFT that represents the node's staking.

Token use and type: nETH is a reward-bearing token that accrues value over time.

NodeDAO provides nETH that allows validators to access liquidity or exit without the need to queue. Similar to stETH, nETH can be transferred on the secondary market. Another option is called vNFT. The vNFT is minted when an individual validator joins the network, and it represents the 32 ETH in a node.

Commission/fee: NodeDAO allocates 10% of execution layer income to the NodeDAO treasury, 20% of execution layer income to the operator and the rest to the stakers.

Node operators: Being a permissionless network, node operators can join either through ChainUp Cloud and XHash or individually. NodeDAO requires 1.1 ETH as collateral to start a node, which is odd, considering that according to Stader, 4 ETH are necessary to cover the majority of slashing risks.



Stakehouse – Blockswap

Summary: Stakehouse protocol is a smart contract-based Staked ETH operating system for programmable staking. Using state replication, the protocol maintains an immutable record of continuous individual validator balances. All smart contracts including the state replication are a ground-up new design that allows for intent-based cross-domain by synching the consensus layer deposit with execution layer derivatives.

Stakehouse is a primitive which is the basis of many Ethereum applications including liquid staking, multichain ETH staking, MEV management, Blockswap Cloud, LSD as a service, and an Ethereum staking CRM. It is also natively compliant with all Ethereum infrastructure, execution & consensus clients, and DVT, and does not require a protocol upgrade.

Current applications of Stakehouse:

• Solo/Institutional Stakers: Stakehouse provides NAV tracking and UX for easy staking with key generation, portfolio management & customization, DeFi compatibility, and no pooling of assets.

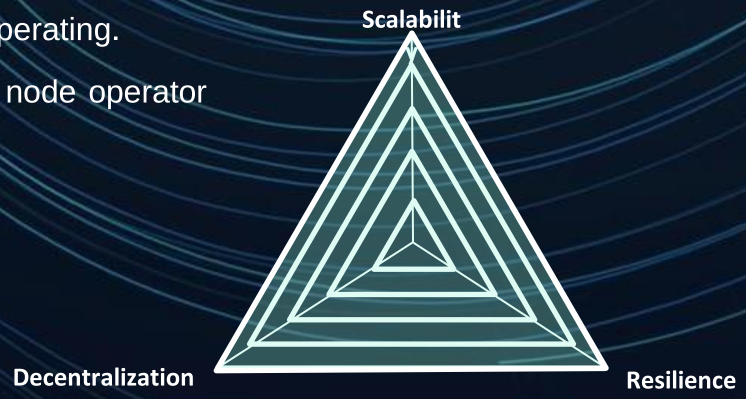
• LSD Networks: Three staking options including MEV Staking, Protected Staking, and Node Operator Staking.

• LSD as a Service: Users can create their own LSD Network and collect a commission using the Stakehouse smart contracts. It includes fully customizable with KYC and token gating.

• Fren Delegation: Enables ETH stakers to liquid stake and provide ETH to a specific validator. This can be a tool for influencers and community members to get liquidity sourced specifically for their validator.

• Compound Staking: Stakehouse staking allows node operators to compound the number of validators they are operating.

• Stakehouse Monitoring: Providing 100% accountability and tracking of staked ETH movements complete with node operator health, MEV rewards, issuance, and index performance.



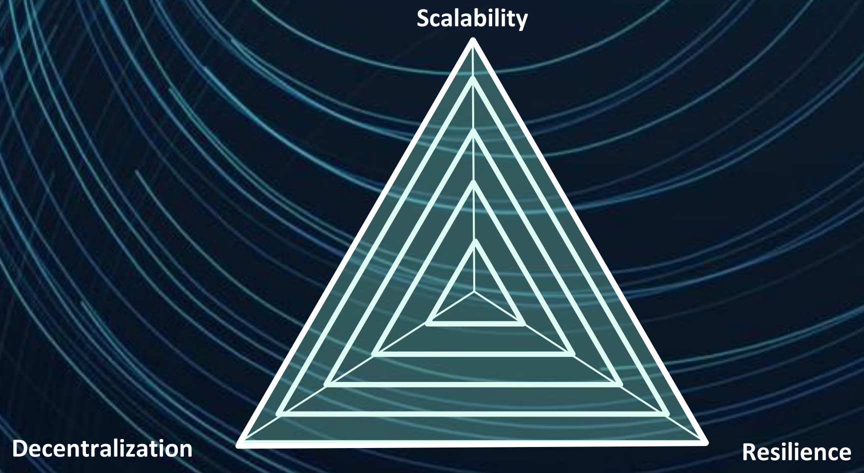
Stakehouse – Blockswap

Token use and type: dETH - Derivative ETH always maintains 1:1 with ETH in a validator. It earns a full validator's staking rewards on only 24 dETH; Up to 33% more than the staking rate.

SLOT Tokens - Represent validator ownership and collect all MEV and tips on only 8 tokens and offer up to a 400% increase MEV on a per ETH basis.

Commission/fee: Stakhouse collects 0 commissions, but LSD owners can set whatever commission they want.

Node operators: Up to the LSD Network, many are permissionless. Stakehouse is 100% compatible with all Ethereum infrastructure, including clients and DVT out of the box.



HASHKEY Capital

Conclusion

There’s fierce competition to gain market share across the Ethereum LSD protocol. The LSD protocols covered in this section of the report try to attract users in different manners: from UI/UX/convenience, lower fees, capital efficiency, integrations, and decentralization.

We have seen that the community values decentralization and that’s probably one of the reasons why RocketPool is the fastest growing LSD protocol post Shanghai. However, it seems that convenience is also a great selling point. This is probably the reason why centralized exchanges like Coinbase, Binance and Kraken have also a significant share of the Ethereum staking market.

Most of the LSD protocols covered in this section are actively working on additional integrations, better user experience, better decentralization (almost all are planning to implement permissionless nodes and DVT) and better capital efficiency.

This is definitely a sector to keep an eye on. As we covered in the report “Unlocking The Potential Of LSD,” The LSD market is prone to grow and engulf billions of dollars in market capitalization.

Disclaimer

The information contained in this document has been compiled by HashKey Group (as defined below) from sources believed to be reliable, but no representation or warranty express or implied is made by HashKey Group, its affiliates or any other person as to its fairness, reasonableness, reliability, accuracy, completeness or correctness. All illustrations, examples or forward-looking information (if any) contained in this document have been provided in good faith for illustrative purposes only as of the date of this document, and are not intended to serve as, and must not be relied upon as, a guarantee, an assurance, a prediction or a definitive statement of fact or probability. Whilst efforts are made to ensure the accuracy and completeness of the information contained in this document at the time of publication, errors or omissions may occur. Past performance is not a guide to future performance, future returns are not guaranteed, and a loss of original capital may occur. HashKey Group reserves the right to correct any errors or omissions, and to change or update information at any time without prior notice.

Each legal jurisdiction has its own laws regulating the types of investments and/or services which may be offered to its residents and/or in its jurisdiction, as well as the process for doing so. As a result, certain investment products or services discussed in this document may not be eligible for sale or offered in some jurisdictions. This document is not an offer to sell or a solicitation of an offer to purchase any investments or services. Unless otherwise specified, HashKey Group does not hold itself out to be licensed to carry on regulated activities in any jurisdiction. Additionally, providing this material is not, and under no circumstances should be construed to act as a regulated business in any jurisdiction by any person or company that is not legally permitted to carry on such regulated business in that jurisdiction.

Nothing in this document constitutes legal, accounting, or tax advice, and you are advised to seek independent legal, tax and accounting advice prior to acting upon anything contained in this document. The contents of this material have not been reviewed by any regulatory authority. Investors are advised to exercise caution in relation to any investments or services in relation to this document. If you are in doubt about any of the contents of this material, you should obtain independent professional advice.

To the full extent permitted by law, neither HashKey Group nor any of its affiliates accepts any liability whatsoever for any direct or consequential loss arising from any use of this document or the information contained herein. No information contained in this document may be reproduced or copied by any means without the prior written consent of HashKey Group.

“HashKey Group” is a brand name to describe any one or more entities of the group companies composed of HashKey Digital Asset Group Limited and its Affiliates.

HASHKEY
Capital

hashkey.capital | ir@hashkey.com