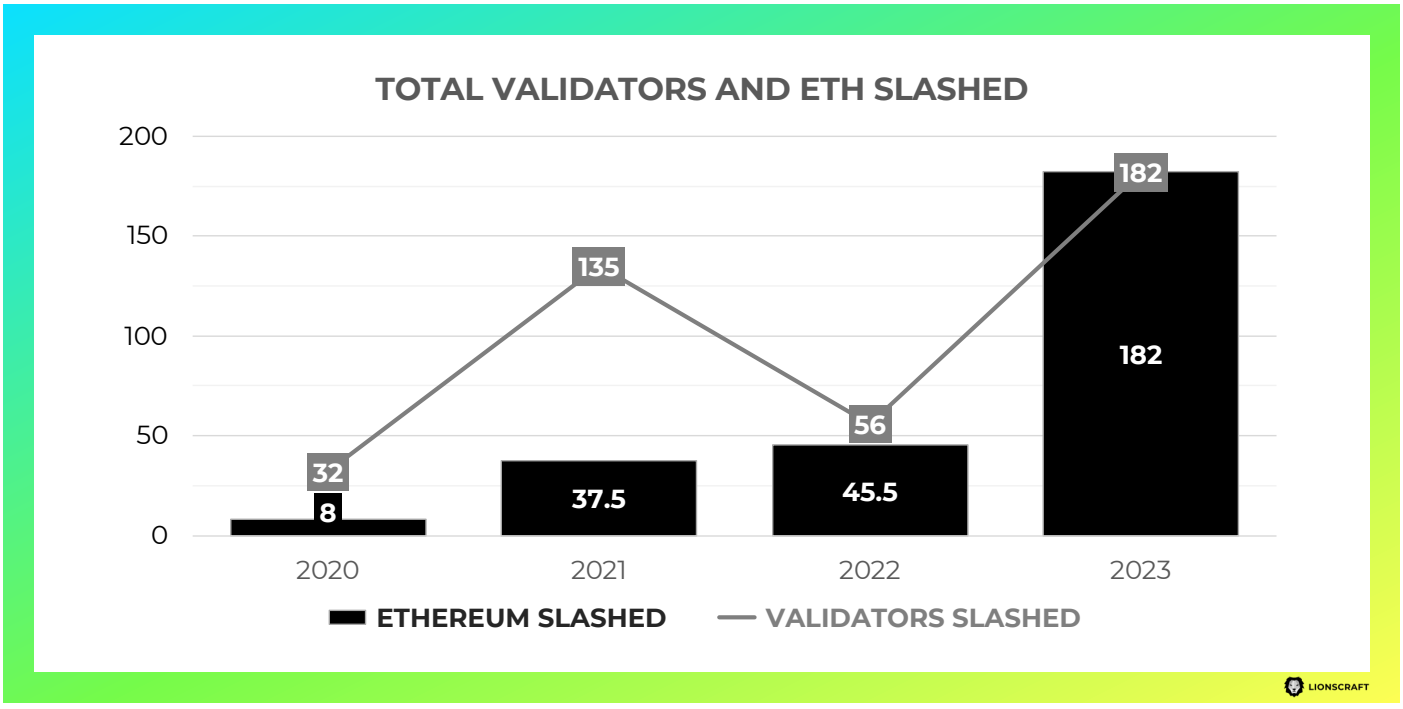
THE 2023 ETHEREUM SLASHING REVIEW

Evolving Landscape, Evolving Risks



In 2023, the Ethereum network experienced remarkable growth, with nearly 400,000 new validators joining the network and staking 13 million ETH, worth USD $49.4 billion in today's prices[i]. This was a 45% increase in the validator pool, pushing the total number of Ethereum validators to more than 900,000 globally. This expansion, as could be expected, was paralleled with an increase in slashing incidents with 182 validators slashed in 2023 – almost half of the 405 total validators slashed since Ethereum transitioned to Proof-of-Stake in 2020.



Notably, direct penalties—ETH burned from a slashed validator—have also increased since 2020. While the number of validators slashed in 2023 was 35% higher than in 2021,

the volume of ETH slashed increased over 380% between 2021 to 2023. This was specifically due to the change in the direct penalty amount implemented in the Altair upgrade in October 2021, where the direct slashing penalty was increased from 0.25 ETH to 0.5 ETH per slashed validator. The subsequent Bellatrix hard fork in September 2022 also saw to another increase, where the direct penalty was now set to 1 ETH per slashed validator. Despite the increase in overall slashing, the average risk of a validator being slashed remains quite low at 0.004%[ii].

WHY DID THE SLASHES OCCUR?

Over 75% of the slashings in 2023 occurred during four Major Events. These Major Events are incidents where more than 10 validators were consecutively slashed within a single period, typically within a few epochs from each other.

MAJOR SLASHING EVENT - 11 ETH SLASHED

In April 2023, 11 validators faced slashing due to a chain of events, initiated by misleading confirmation of key deletion during migration to a new cluster. This process involved the unintended re-import of deleted keys due to a Prysm software bug. The original assumption was that the keys in the original cluster were properly deleted. However, when the Prysm clients restarted after an update a few days later, the supposedly deleted keys were unexpectedly brought back into the original cluster. This led to double signing from both the original and migrated clusters. Prysmatic Labs confirmed this re-import as a bug, which has since been fixed.

MAJOR SLASHING EVENT - 20 ETH SLASHED

In October 2023, a connectivity issue in the primary data center prompted a fallback procedure, where multiple validator instances were spun up. The initial instance and a manually activated fallback instance, were directed to a single Web3 Signer. Unfortunately, the Web3 Signer did not have its slashing database enabled, leading to the occurrence of double signing and the subsequent slashing of 20 validators.

ADDITIONAL MAJOR SLASHING EVENTS - 111 ETH SLASHED

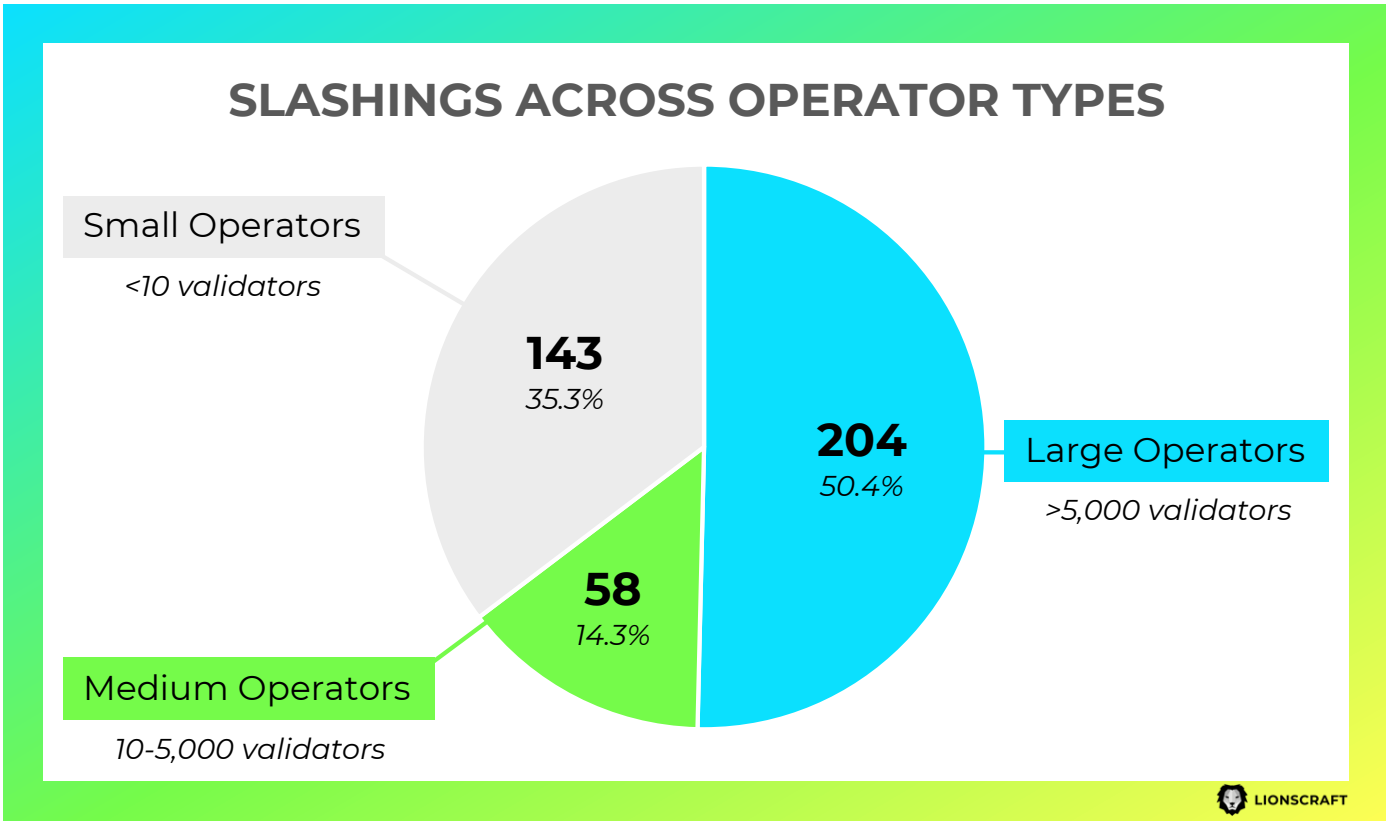
Beyond the April and October 2023 slashing incidents, two further Major Events have occurred: 12 ETH slashed in August 2023 (details undisclosed) and 99 ETH slashed in November 2023 due to human error during new validator deployment.

SLASHING INCIDENT: MALICIOUS ATTACK, 1 ETH SLASHED BUT $25M GAINED

While most slashing incidents on the Ethereum network were due to inadvertent errors, a notable case in April 2023 highlighted how slashing could be intentionally used for financial gain. MEV (Maximal Extractable Value) involves extracting extra profit by reordering transactions within a block, often exploited by automated MEV bots. These bots utilize tactics like sandwich attacks to manipulate transaction prices to their advantage, causing losses to targeted transactions.

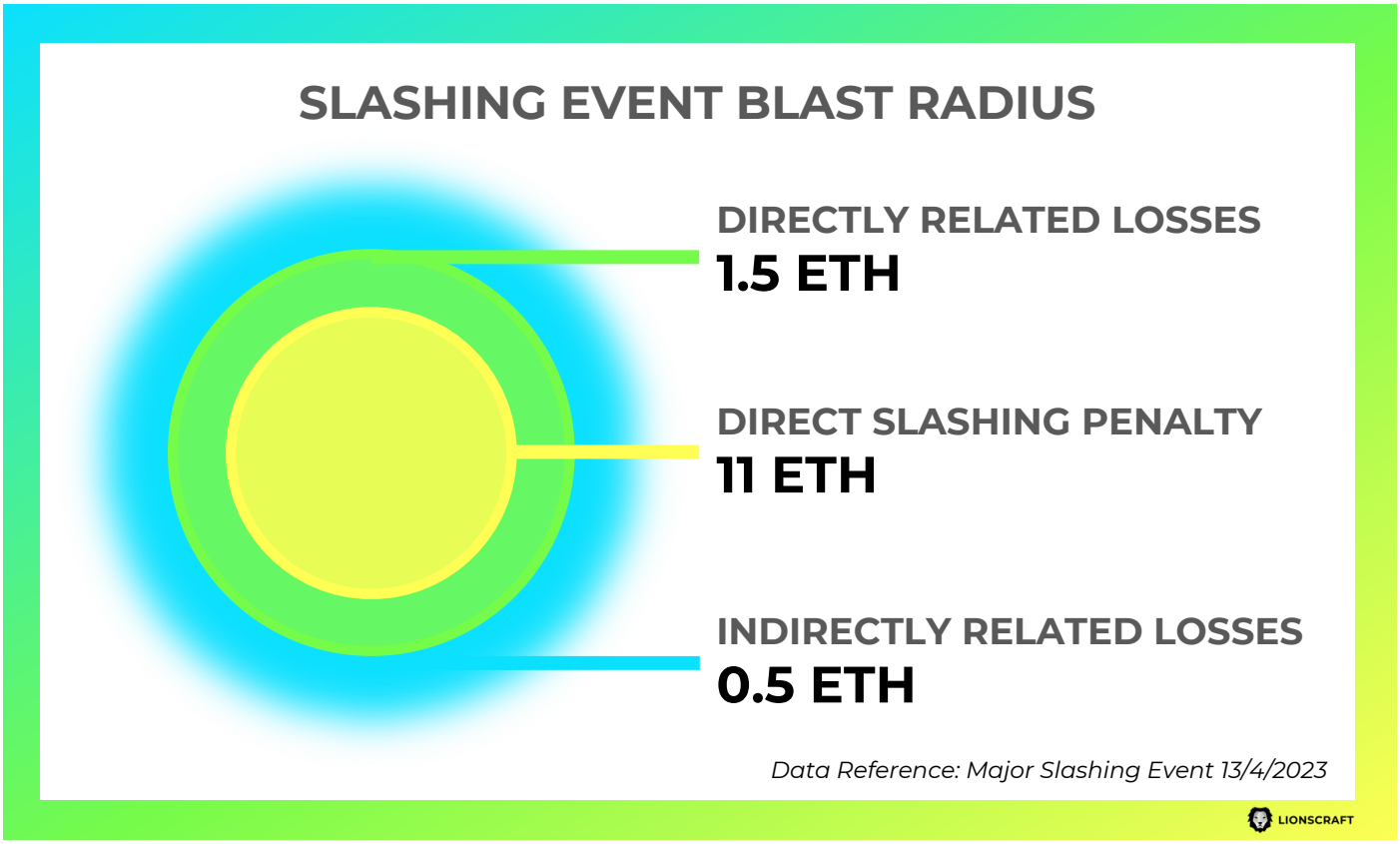
During the incident, attackers targeted MEV bots by exploiting a flaw in the MEV-Boost relay system. By strategically deploying at least 16 validators nearly a month before, the attackers increased their chances of being chosen as a block proposer. Once chosen, they sent bait transactions to entice MEV bots into executing sandwich attacks. Exploiting the relay flaw by sending a signed but invalid block header, the attackers gained access to the block content. This allowed them to extract transactions and create their own block which they re-signed then broadcasted to the network. Their new transactions essentially sandwich-attacked the bots' sandwich attack, earning them $25 million at the cost of being slashed 1 ETH for proposer equivocation.

WHO GOT SLASHED?



Across the lifetime of the network, it was found that just over half of all slashings were linked to either large operators (managing over 5,000 validators), or small operators (managing less than 10 validators). Medium-sized operators (managing between 10 to 5,000 thousand validators) seemed less frequently involved in slashing incidents.

The fact that large operators manage significantly more validators means that a single error could have far-reaching consequences. Additionally, large operators tend to experience cascading losses beyond direct slashing penalties. This broader impact, referred to here as the "**Slashing Event Blast Radius**" represents a ripple effect of additional losses that may not be immediately evident.



The Slashing Event Blast Radius comprises of three layers. In addition to the fixed Direct Slashing Penalty of 1 ETH per validator slashed, there are two further types of losses: Directly Related Losses and Indirectly Related Losses. Directly Related Losses include penalties due to missed attestations during the validator exit period, and opportunity costs stemming from missed attestation and proposal rewards during that time. As an illustration, in the April 2023 Major Event where 11 validators were slashed, Directly Related Losses were calculated to be an extra 1.48 ETH, on top of the 11 ETH Direct Penalty.

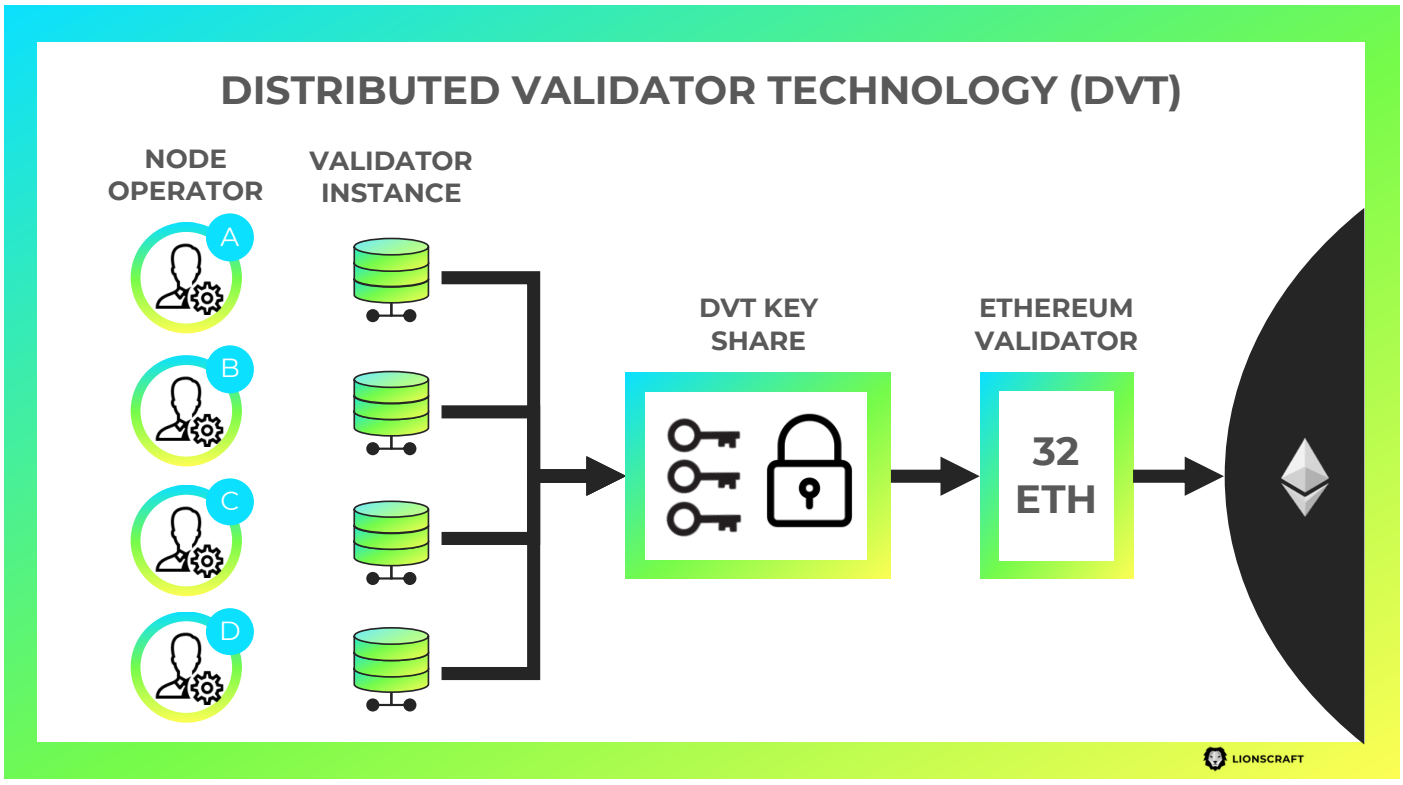
Furthermore, operators may incur Indirectly Related Losses that could arise from, for example, emergency shutdown of related validator clusters while managing the incident, this would result in a loss of potential rewards while these validators are offline. The extent of these indirect costs varies depending on factors such as the size of the cluster and the duration of the shutdown. For example, during the April 2023 Major Event, a cluster of 1,000 validators was shut down, leading to 0.48 ETH of Indirect Losses.

In addition to these financial costs, slashings also have a reputational impact on the operators. This could manifest as a reduction in future staking delegation, due to a decline in the trust from current and prospective stakers, and higher premiums or difficulty in obtaining slashing insurance. Although difficult to measure, these costs could significantly affect the operator's position within the industry.

MITIGATING SLASHING RISK AND DAMAGE

Several initiatives have been developed to address slashing risks and their subsequent effects, which can be organized into three broad spheres: technical, procedural and business solutions.

TECHNICAL SOLUTION: DISTRIBUTED VALIDATOR TECHNOLOGY



Distributed Validator Technology (DVT) transforms Ethereum node management by distributing validator keys and responsibilities among multiple node operators, thereby reducing centralization, and enhancing security. This decentralization minimizes the risk of slashing, as it eliminates the vulnerability of a single point of failure holding the private key. Instead, DVT employs a collaborative approach where multiple parties sign node messages, enhancing efficiency and resilience.

However, while DVT mitigates centralization risks, it also introduces new challenges. Validators now must incorporate another software into their existing stack of tools and technologies. This additional software, DVT, adds to the complexity of managing the node operations, alongside existing components such as consensus and execution clients, web3 signers, slashing databases, and monitoring tools.

Obol and SSV Network are the two leading projects developing DVT. In November 2023, Lido, the largest liquid staking provider on the Ethereum network, approved a proposal to incorporate the first DVT module from Obol and SSV Network into their operator set.

PROCEDURAL SOLUTION: DOCUMENTATION & FRAMEWORKS

In addition to technological advancements, various initiatives are underway to improve operational performance and mitigate slashing risks through procedural and preventative measures. One approach involves the development of comprehensive public knowledge bases and standardized best practices for node operations. The EthStaker community, boasting over 50,000 members, serves as an exemplary model in this regard, offering guidance, education, and resources tailored to stakers' needs. Furthermore, platforms like Lido, in collaboration with Lionscraft, have introduced dedicated frameworks such as D.U.C.K. (Distributed Utilization of Configurations and Knowledge) specifically designed for their node operators. These frameworks provide open-source knowledge bases encompassing risk frameworks and mitigation strategies. By empowering stakers and node operators with the necessary knowledge and tools, these initiatives contribute to the overall security and integrity of the Ethereum staking ecosystem.

BUSINESS SOLUTION: SLASHING INSURANCE

Moreover, there are business and financial tactics available to mitigate the consequences of slashings if they occur. One such strategy involves acquiring slashing insurance, which can provide financial mitigation in the aftermath of slashings. This insurance offers reassurance to stakers, ensuring compensation for any losses resulting from slashing events. Typically, operators and protocols either self-insure or seek coverage from external providers. For example, Lido DAO has chosen self-insurance through their Treasury Fund, while brokers like Aon can help operators obtain slashing coverage from providers like such as MunichRe and Chainproof who offer slashing insurance.

SHIFTING LANDSCAPE OF ETHEREUM SLASHING

The slashing landscape on the Ethereum is evolving due to several ongoing developments. This section explores two key areas potentially impacting staking dynamics: Restaking and EIP-7251.

RESTAKING AND INCREASED SLASHING RISK

Restaking is a new strategy in the Ethereum staking landscape that aims to boost returns for existing stakers. It does this by leveraging liquid staking tokens, representing already staked ETH, to bolster the security of other protocols and blockchain networks beyond the Ethereum ecosystem. Restaking offers several benefits:

- Enhanced returns: Stakers can accrue additional rewards on top of their initial staking yield. Essentially, their staked ETH performs a dual function, securing both the Ethereum network and other protocols simultaneously.
- Improved ecosystem efficiency: By utilizing existing security resources, i.e. staked ETH, restaking eliminates the need for individual applications and protocols to build their own security measures

However, restaking also comes with increased risks. The most significant is the additional exposure to new slashing conditions. Unlike staking solely on Ethereum, restaking exposes staked ETH to the unique slashing rules of the additional protocols it secures. Currently, EigenLayer is the leading protocol on Ethereum that offers restaking services. It is important to acknowledge that restaking remains a relatively new concept, and its long-term implications are still under active discussion within the Ethereum community.

EIP-7251: POTENTIAL IMPACT ON VALIDATOR SET SIZE AND NETWORK OVERHEAD

Drafted in late 2023, EIP-7251 proposes increasing the maximum amount of ETH that could be staked per validator, from 32 ETH to 2048 ETH. This change aims to:

- Consolidate operations: Large node operators could manage fewer validators, simplifying their operations.
- Benefit solo stakers: Solo stakers could benefit from compounded rewards and greater staking flexibility.

By raising the cap to 2048 ETH, EIP-7251 seeks to reduce the validator set size, potentially lowering network overhead in several ways, including:

- Reducing the number of peer-to-peer messages.
- Decreasing the number of signatures needing aggregation.
- Minimizing the memory footprint of the Beacon State.

The initial proposal considered removing the initial slashing penalty to incentivize consolidation. However, ongoing discussions within the community suggest a potential alternative: fixing the initial penalty to a constant amount or applying a sublinear scaling mechanism. It's important to note that EIP-7251 is still under community discussion and would require a hard fork if implemented.

These developments highlight the evolving nature of the Ethereum slashing landscape. Restaking introduces additional risk considerations, while EIP-7251, if implemented, could significantly impact the validator set size and network efficiency.

SUMMARY

The 2023 Ethereum Slashing Review casts light on the evolving complexities of the Ethereum network. It highlights a significant increase in both the number of validators joining the network and the frequency of slashing incidents. This trend particularly impacts large operators, who face the brunt of these occurrences.

The review introduces the Slashing Event Blast Radius, referring to the cascade of losses that extend beyond the direct slashing penalty. This includes losses in missed rewards, emergency shutdown costs, and reputational damage, all of which can significantly impact affected operators.

Furthermore, the review outlines several approaches to mitigate both the risk of slashings and their impact. These approaches encompass technical solutions, business strategies, and procedural mechanisms. Finally, it highlights emerging initiatives like restaking and EIP-7251, which have the potential to significantly reshape the slashing landscape and its implications for network participants.

These developments underscore the rapidly evolving complexity of the Ethereum network. The review emphasizes the crucial role of node operators in remaining vigilant and well-informed to navigate the changing landscape and effectively manage their staking activities.

About Lionscraft

Lionscraft was founded in the midst of the digital revolution. We are a dynamic Web3 strategy and technology firm, driving growth and innovation in organizations by harnessing the power of Web3. Lionscraft provides cutting-edge business and technical solutions, empowering organizations to navigate the complex and fast-evolving Web3 landscape. Together with our diverse range of clients – from Web3 industry leaders to global powerhouses in finance, technology, and communications, we are shaping the future of Web3.

We offer bespoke consulting, knowledge and training on Node Operations, Slashing and Risk Management for Staking Infrastructure.

Explore more about Lionscraft's vision and offerings on our website and social media.

https://www.lionscraft.io
https://x.com/Lionscraft_io
https://www.linkedin.com/company/lionscraft

[i] At Epoch 253237 and price of ETH used to calculate the $49.4 billion is $3,800 on 6/3/2024
[ii] Overall average of number of slashings per month for each average number of validators per month