ADAN

Report on Staking

overview and regulatory analysis

Staking plays a crucial role in securing the functionality and integrity of blockchain networks, enhancing transaction speed and throughput by aligning participant incentives and contributing to the overall sustainability of these innovative systems.

This report aims to elucidate the concept of staking, which is a fundamental component of blockchain technology, outlining how it works and providing an overview of current regulatory standards.

Adan is appreciative of the opportunity to engage in discussions about staking, and we hope that our comments on this document will be useful to the European regulators.

Executive Summary

1. What is staking?

To effectively explain the concept of staking, first, it is essential to understand blockchain technology, as staking is intrinsically linked to the functioning of blockchain networks.

At its core, blockchain is a form of Distributed Ledger Technology (DLT) that stores information in a chain of blocks. New blocks of data chronologically added to the ledger include a unique digital fingerprint called a hash also known as signature (an algorithm) whose creation depends on the hash of the previous block and the data it contains. As each block cannot be altered without manipulating the hash of all previous blocks, the ledger is strengthened with each new block addition. If the block's data is manipulated, the hash will change and will not match the hash stored in the subsequent block. This makes it possible to detect if someone attempts to tamper with the information stored in the blockchain, providing greater resilience to failures and attacks.

Every blockchain network employs a unique validation process, called “consensus mechanism”, to incentivize nodes to contribute resources to the network and ensure the successful settlement of transactions (or new recording of data) for network users.

The first blockchain consensus mechanism, used by the Bitcoin network, was Proof of Work. Proof of Work involves “miners” solving a complex mathematical puzzle by brute force, thus demonstrating “proof” that they have undertaken non-forgeable computational work. Proof of Stake involves validators pledging assets to the network similar to a form of collateral instead of miners undertaking computational work. Fundamentally, Proof of Stake (PoS) is a type of consensus mechanism for processing transactions and creating new blocks in a blockchain which enables information and value to be transmitted and stored without a centralized control body or trusted third party. The trusted third party is substituted by a distributed group of users who operate computers (“nodes”) of the network, which run all or part of the software. These nodes perform as “validators” of recorded and new information.

In simple terms, Proof of Stake (PoS) is a type of blockchain consensus system that enables network participants to 1) validate the information stored on the blockchain, helping to prevent any attempts to alter it, and 2) ensure that the new recording of data (or validate transactions) in the ledger adding them to the blockchain by grouping them together in a new block.

A. What Validators Validate in PoS?

Validators validate **transactions** proposed to be added to the blockchain, attesting that the transactions are correctly signed, that the sender has sufficient balance, and that there is no duplication.

Validators also validate entire **blocks** of transactions, confirming that the block adheres to the network's rules, including the correct structure, the inclusion of valid transactions, and the proper linking to the previous block.

Likewise, validators ensure that the proposed blocks comply with the specific **consensus rules** that rule the network, such as block size limits[1], gas limits (in Ethereum), and other protocol-specific requirements.

[1] Blockchain block size limits refer to the maximum amount of data that can be included in a single block of transactions on a blockchain network. Different blockchains may have varying block size limits, depending on their design and specific requirements.

B. How does the PoS Process Work?

To be eligible to validate transactions and create new blocks on a Proof of Stake network, validators must deposit or immobilize a certain quantity of crypto-assets native to the Blockchain. Most blockchains have a relatively high minimum staking threshold to become a validator — Ethereum, for instance, requires validators to stake at least 32 ETH. The amount of stake often influences the chances of being selected as validators. In return, validators receive their immobilized assets and rewards in the form of these same crypto-assets. In the given example, the validator would receive 32 ETH along with additional ETH as reward.

The selection of validators occurs through an algorithm that randomly chooses a validator group over a given period of time from all those who have staked (or locked up) a minimum amount of crypto in a smart contract. This selection process can vary between different PoS implementations. Several factors can influence the likelihood of the selection of validators. The most significant is the amount of crypto-assets that have been staked. The more assets are committed to the network the higher chances to be selected. This is because many PoS algorithms use a weighted random selection process where validators with larger stake have greater possibilities of being chosen. However, PoS networks might use other factors. Some networks incorporate a reputation system that evaluates validators based on their performance and reliability. Validators with a stronger "reputation" may be favored for the selection. Other PoS favor active participation in the network- such as validating transactions but also responding to governance proposals, etc- or favor the performance, where validators that maintain high uptime and perform well in terms of block validation are more likely to be selected. Others simply incorporate elements of randomness.

Once selected, the validator proposes (forges) a new block grouping the transactions together, and determines a new state for the ledger. The block is sent to other validators (known as "controllers") which verify the accuracy of the integrity of the block, add it to their own database, and distribute it over the network.

Validators maintain a copy of the blockchain ledger, which reflects the current state of all transactions and balances as agreed upon by all participants in the network. Each validator receives updates about the ledger status, ensuring they have the most recent and accurate information. This ledger is distributed across all nodes in the network, meaning every participant has a copy of the entire blockchain.

The other selected validators will make use of this copy to review the proposed block. They validate the transactions and the block structure (see previous section). If they "agree" that the block is valid, they cast votes to confirm it. The block is then added to the blockchain once a sufficient number of votes (a supermajority) is reached.

Once a block is created, it is propagated throughout the network. Other validators and nodes receive the new block and verify its contents, ensuring that it adheres to the consensus rules. If the block is deemed valid, it is added to the blockchain and the state of the ledger is updated across all nodes. Following verification, the transactions are executed, resulting in changes to the blockchain's virtual machine state. This execution updates account balances, records new transactions, and modifies the overall state of the ledger. The results of these calculations are then committed to the blockchain, making them permanently recorded and unalterable.

Once the block is added to the chain, in return, validators earn rewards (usually in the form of transaction fees and newly minted tokens- "gas fees"), although reward structures vary.

Validators are incentivised to maintain the integrity and security of the network as they receive rewards in return for their participation in block proposing and attestation. For certain PoS chains, they are disincentivised from breaching protocol rules as they stake or “lock up” assets and they risk losing their a portion of their “stake” or rewards if they break specific protocol rules either negligently or maliciously eg falsifying blocks or double signing. Furthermore, a sufficiently diverse set of validators minimizes the risks of centralized control, lessens the impact of client bugs on the network’s health, and mitigates security threats.

By staking their tokens, users are motivated to support network stability. As validators, they contribute to transaction verification and processing, mitigating the risk of fraudulent activities. A larger pool of staked tokens enhances network decentralization and security, as a potential attacker would require control over a substantial portion to compromise the system, a challenging and expensive undertaking.

Furthermore, Staking enhances the scalability and efficiency of PoS networks. With validators incentivized to participate, transactions are processed at a faster pace than traditional proof-of-work systems, resulting in quicker block times and increased transaction throughput, fostering wider adoption of blockchain technology. Moreover, staking promotes greater sustainability of blockchain networks, requiring significantly less energy compared to proof-of-work mechanisms, making it a more environmentally friendly option for the future.

Europe has emerged [2]as a significant hub for staking on the Ethereum blockchain, with a substantial number of Ethereum nodes operated in EU countries. This concentration of nodes in Europe underscores the region's pivotal role in the Ethereum network's infrastructure and governance.

C. Locking Up Assets in Smart Contracts

By leveraging smart contracts, the process becomes automated, secure, and transparent, fostering trust among participants in the blockchain ecosystem. This system contributes to the overall security and stability of the network.

A smart contract is a computer program stored in and executed in the blockchain. Smart contracts are used for the automated execution of actions based on “if- then conditional” logic pre-programmed through codes. The Smart contract will execute the agreed task or action when the coded conditions and criteria are met.

The use of smart contracts in the lock-up process enhances trust in the staking mechanism. Since the rules are encoded in the contract and executed automatically, there is less reliance on a single party, promoting decentralization.

In the context of a staking process, the validator interacts with smart contracts which are specifically designed for staking. This smart contract governs the staking process, including the rules for locking up assets, rewards distribution, and penalties for misbehavior, according to the pre-defined blockchain protocol rules.

First, the validator initiates a transaction to transfer their crypto-assets to the staking smart contract. This transaction specifies the amount of assets to be locked and may include additional parameters, such as the duration of the lock-up. Upon receiving the transaction, the smart contract executes the lock-up process. The smart contract then records the amount of

[2] https://dune.com/chainbound/geolocating-validators Last seen 25/09/2024

crypto-assets being staked and associates it with the validator's address. In parallel, the smart contract updates its internal state to reflect the locked assets, ensuring that these assets cannot be used elsewhere in the network.

While the assets are locked in the smart contract, validators earn rewards for their participation in the network. These rewards are typically distributed in the form of additional crypto-assets, which is also managed by the smart contract. In some systems, rewards can be automatically re-staked, meaning that they are added to the validator's stake to increase the potential future rewards.

However, validators might decide to withdraw their staked assets, for which they must initiate an unstaking process through the smart contract. This typically involves sending a transaction to the smart contract indicating the desire to withdraw.

Many networks implement a waiting period for un-staking to prevent sudden withdrawals that could destabilize the network. During this time, the validator may continue to earn rewards, but the assets remain locked. After the waiting period, the validator can withdraw their original staked assets along with any earned rewards. The smart contract updates its state to reflect the withdrawal, and the assets are transferred back to the validator's wallet.

To ensure the security of the lock-up process, staking smart contracts are often audited by third-party firms. This helps identify vulnerabilities and ensures that the contract behaves as intended.

2. Staking taxonomy: Direct vs indirect staking

Subjects that participate in a PoS consensus mechanism broadly fall into two categories:

- Validators: node operators that verify transactions and create new blocks.
- Delegators: users who lock up a stake of their crypto for a specified period and delegate it to validators to secure and process new transactions on the blockchain. The delegator role enables users to participate in staking without having to run the validator software themselves.

Staking can be carried out either directly or indirectly. In this context, we can differentiate between solo and indirect staking.

A. Solo staking

Solo or technical staking refers to invidual'sdirect participation in the staking operations without the reliance on a third-party intermediary. The individual typically operates a validator node, which requires a dedicated commitment, including the maintenance of adequate hardware and network connectivity for the validation and proposal of blocks. The individual has full control over the staked assets and the validator node.

B. Indirect staking

In indirect staking, the delegator does not run the software for validation directly. Indirect staking involves crypto-assets holders delegating staking activities on the network to a validator,. The delegator can earn rewards without the technical complexity of having to run and cost associtated with running a validator.

Different modalities of indirect staking

As we will see further below, it is important to note that there are modalities of indirect staking. 1. Where users retain control of their private keys while delegating their assets to validators. 2. Delegators entrust their assets to a third-party service provider eg a custodian, who manages the staking process on their behalf.

→ **Delegated staking - Non Custodial** allows users to stake their crypto-assets without relinquishing ownership or custody to a third party. Instead, users delegate their staking rights to a validator node while maintaining control over their crypto assets in their self-hosted wallets.

→ **Delegated staking - Custodial** allows users to stake their assets from a custodial solution offered by a third party. Users still control and elect whether to stake or not but control of private keys / assets is handled by the custodian. Staking can therefore be seen as an ancillary service to the custodial activities provided by the custodian.

Models may vary but providing access to staking services also known as **Staking-as-a-Service (StaaS)** can be done on a custodial or noncustodial basis. If done in a custodial context the custodian custody and control of the tokens themselves. But it is crucial to highlight that this custodial transfer is a result of the firms' status as a custodian and is not related to, or indeed necessary for, staking to take place. StaaS providers simplify the staking process for individuals, relieving them of technical complexities. In exchange, they typically charge a fee, often a percentage of the staking rewards.

It is important to note that StaaS does not necessarily involve custodial services by the intermediary. Users can indeed transfer their assets to the StaaS provider who will manage the staking on their behalf. In these cases, users do not retain control of their private keys. However, in other StaaS business models, users retain control of their private keys while delegating their staking to the StaaS provider, often through smart contracts.

→ In **pooled staking**, users delegate their assets to a staking pool. Instead of staking individually, users contribute their assets to a shared pool by a staking service or a pool operator. Pooled staking lowers the barrier to entry eg. where a user does not have 32ETH to deploy for validation purposes. Rewards from pooled staking are distributed among participants based on their staked assets. It benefits participants as it allows individuals with limited resources to stake independently, to participate in staking. There are two modalities of pooled staking. One where users relinquish control over the private keys to the pool operator. This implies that the pool operator holds and manages the assets on behalf of the delegator. Some staking pools operate on a non-custodial basis, allowing users to retain control over their private keys. In this case, users delegate their staking rights without transferring their custody of their assets.

Information disclosure to delegators

Blockchains like Ethereum have taken steps to enhance the legal framework surrounding staking activities. They have developed comprehensive contractual documentation that outlines the rights and responsibilities of all parties involved in the staking process. This legal certainty not only fosters trust among participants but also establishes clear guidelines for the operation of staking services. Such documentation can include terms related to: slashing conditions, rewards distribution (how staking rewards are calculated, distributed, and distribution frequency), fee structures, consumer protection, and mechanisms for addressing disputes.

This information might be in the blockchains' whitepapers, technical documentation, and user guides on their official websites. The information can also be provided at the time of staking or when users are considering staking. Platforms might also require users to review and accept terms and conditions before proceeding with staking. Notifications may also be provided when rewards are distributed or when there are updates on validator performance or any changes that may affect delegators.

In the context of staking rewards, transparency is a critical factor that can greatly influence investor confidence and decision-making. Certain blockchains have recognized this need and have implemented mechanisms to publish key performance indicators for each validator. One of the most important metrics is the percentage of availability, which reflects how often a validator is online and actively participating in the network. A high availability percentage indicates that a validator is consistently operational, which is essential for maintaining network security and ensuring that stakers receive their rewards without interruption.

In addition to availability metrics, these blockchains also disclose information about any past misbehaviors by validators, particularly those that have led to slashing penalties. By making this information publicly accessible, blockchains empower investors to assess the reliability and trustworthiness of validators. This approach not only promotes responsible validator behavior but also encourages broader participation in staking, ultimately contributing to the overall health and stability of the blockchain ecosystem.

3. Risks

A. Theft or loss of assets and rewards

This is a risk shared by solo and indirect staking modalities. Delegators are exposed to traditional cyber risks like hacking and phishing, which can result in the loss or theft of their delegated crypto-assets and rewards prior to their return. Delegators might also encounter scenarios where validators fail to pay all or part of their earned rewards based on the amount of delegated crypto-assets. This risk primarily arises when the blockchain protocol interacts solely with the validator. Such situations could occur due to imprecise agreements or the absence of a contract between the delegator and validator that specifies a method for calculating reward distribution.

However, this risk is mitigated when rewards are paid directly from the blockchain protocol to delegators.

However, in custodial StaaS this risk is mitigated thanks to MICA rules, which mandate a contractual relationship between CASPs and their clients, obliging the formers to provide in a transparent manner, all the information related to the service. In addition, users will be covered by the liability rules and insurance policy requirements established in MICA.

B. Penalties for failure in the block validation

Slashing is a risk for solo and indirect staking modalities (although it is important to note it is a penalty that only certain PoS chains deploy). The risk of *Slashing* is where a delegator may lose all or part of their staked crypto-assets due to failure in the block validation behavior by the validator. Slashing may be perceived as a consumer protection mechanism rather than a penalty as intends to protect users' staked tokens. Slashing is part of an the incentive mechanism to keep the network secure. *Slashing* prevents a validator from recovering their initial stake.

However, as we will further explain in the regulatory section, in delegated staking, CASPs might provide staking products as an ancillary service to the custody and administration of crypto-assets, where the CASP appoints a third party to run as validator and perform the staking activities. The CASP providing custody will adhere to MiCA obligations, thus extending protection to customers in these situations.

Where the CASP acts as the validator and is responsible for the negligent behaviour, the CASP is subject to the liability rules provided in MICA. In addition, the user is covered for the losses under the insurance policy that CASPs must have in place, and will have to restore the lost assets to their clients.

It is worth noting, that slashing is a native risk of Ethereum. However, other blockchains provide different types of mechanisms. Solana for example does not implement slashing, if a validator signs a block with an incorrect hash, they will face penalties by losing the chance to sign and earn rewards for several subsequent blocks. In Cardano "bad" stake pool operators are penalized by forfeiting future staking rewards. Avalanche also does not utilize slashing. Instead, the consequence for downtime or improper behavior is that the network withholds staking rewards at the end of the staking term.

Certain blockchains provide transparency by publishing the percentage of availability for each validator, as well as information regarding any past misbehaviors that may have resulted in slashing penalties. This type of data is invaluable for investors, as it allows them to make informed decisions when selecting validators. By choosing validators with a proven track record of reliability and minimal slashing incidents, investors can significantly reduce their risk exposure.

Absence of restitution for the underlying crypto-assets in liquid staking (LSTs)

Liquid staking introduces unique risks for end users, including the potential inability to regain access to their underlying crypto assets in return for their Liquid Staking Tokens (LSTs) at the end of the staking period. Despite delegating their crypto-assets and receiving an LST as a receipt or certificate of proof of delegation, delegators may lose access to the underlying asset. The risk of this happening will depend in turn on who is issuing the LTS. If it is a centralised party, the risk may include counterparty risks such as misconduct, information security, and bankruptcy. If the LST is issued by a Defi protocol, the counterparty risks will depend on whether there are significant centralisation vectors. If the protocol is truly decentralised, many counterparty risks will be reduced or eliminated but instead, the user will be exposed operational/technical risks in the form of smart contract bugs and hacks risks. Additionally, deppeging is a commonly cited staking risk. End users face the risk of depegging, where the LST loses its fixed 1:1 parity with the underlying crypto-asset. This might happen where, during the staking period, market prices of assets change due to the volatility of the market pricing. It is thus worth noting, that de-pegging is a risk native to secondary market dynamics and not properly linked to the staking process.

It could also occur when withdrawal requests for staked tokens before the unbonding period exceed the capacity of the liquid staking protocol's reserve tokens. When a user wants to withdraw their staked assets, they typically need to initiate a redemption process. This process may involve an unbonding period, where the user may have to wait for a specified period during which their staked assets are locked and cannot be accessed. If the user wants to redeem their LSTs before the unbonding period is complete, they may not receive their original staked assets immediately. Instead, they might receive the protocol's own tokens or a claim on the staked assets, depending on how the protocol is structured. Nevertheless, the situation is circumscribed to the staking period.

A risk arises if many users simultaneously request to redeem their LSTs for the underlying staked assets, and the protocol cannot fulfill these requests due to the unbonding period or insufficient reserves. If users realize that they cannot un-stake their staked assets immediately and must wait for the unbonding period, they may start selling their LSTs in the market. This selling pressure could lead to a decrease in the market price of the LST, causing it to de-peg from the original value of the underlying staked asset, at the time when the asset was staked.

However, it is worth to be noted that, while these risks are present, they rarely materialize in practice.

C. DeFi staking

DeFi protocol staking activities involve the similar risks for investors as those associated with centralized CASPs, such as theft, loss of delegated assets, non-payment of rewards, and slashing. The primary distinction lies in the decentralized nature of DeFi protocols. As argued in D above, if a DeFi protocol has significant centralisation vectors, then it presents many of the same risks as a centralised party (eg if a single individual possesses the ability to change the code and steal assets, then the user is trusting them not to do that). But if a protocol is truly decentralised then it replaces many counterparty risks with operational / technology risk. The absence of liability rules in MICA further differentiates DeFi staking from centralized CASP staking.

4. Regulatory analysis of ancillary services for staking

A. Distinction between Staking/ Financial Activity/ Financial Service (Staking as a Service)

As previously explained, staking is fundamentally a technological operation that contributes to the security and functionality of a blockchain network. It involves participants locking their assets to validate transactions and maintain the integrity of the network. The rewards earned from staking are necessary incentives for users to participate in this process, ensuring that the network remains secure and operational.

Nevertheless, in order to identify the regulatory standards on staking, first, it is paramount to acknowledge the distinction between the technological activity of staking, and a financial service.

Staking is not a financial service. A financial service refers to the various activities provided by a financial institution acting as an intermediary to facilitate the financial activities. Whereas staking is a technical function to secure a network, rewards are a byproduct of this technical function.

Understanding this distinction is vital for regulatory purposes. While staking is essentially a blockchain security function, some business models offer delegating the technical aspects of staking (activities that do not qualify as financial services), as an ancillary service to financial services, which are regulated from 2 angles:

A) Custody and administration of crypto-assets

B) Staking from a technological point of view.

A) Custody and administration of crypto-assets

As seen in the taxonomy section, delegated staking can involve (but not in all cases) custody of crypto-assets by a third party. When staking is ancillary to custody and administration of crypto-assets services, they fall under the scope of relevant regulations. As previously explained, custodial staking services are typically provided by crypto-asset exchanges or custodial wallet providers. Users deposit their coins with the service and the provider stakes on their behalf.

Notably, when using staking services ancillary to custodial services, users transfer ownership of their tokens to the provider. The provider distributes rewards to users, often after deducting a service fee. Custodial staking involves a transfer of ownership. However, many custodial staking services offer insurance or guaranteed returns to mitigate these risks.

Unlike custodial services, non-custodial staking services do not take possession of users' tokens. They provide software that enables users to stake directly from their self-hosted wallets. The service does not have access to user assets and merely facilitates the staking process. This provides users with greater security, control, and autonomy, as they do not need to entrust their assets to a third party. Non-custodial staking is accessible to users with varying technical expertise, allowing them to maintain control over their assets.

A case-by-case analysis is necessary to determine whether a service falls into the custodial or non-custodial staking category.

Differentiating between custodial and non-custodial staking services requires a careful examination of the specific service provider's operations and the degree of control that users retain over their crypto-assets. In the next section, we will analyze the workings of both direct and indirect staking.

→ Custody in Indirect staking

As previously explained, CASPs providing custodial services may also offer ancillary staking services. In such cases, users' crypto-assets are transferred to a CASP-owned wallet that acts as a validator on the blockchain. Thus the CASP provides custody services for both the staked assets and rewards received. In this scenario, the blockchain transfers staking rewards to the CASP's hosted wallet, with no direct interaction with the end user.

Is worth to be noted that, other intermediaries may offer indirect staking without providing custody services. For example, offering the option of delegating from users' self-hosted wallet their crypto-assets to the validation node operated by a validator. In these cases, the intermediary does not retain the crypto-assets, and only allows users to participate in staking through its validator node.

It is paramount to distinguish between the keys associated with running of validator and the private keys of the user over its delegated assets.

In pooled staking, users contribute their assets to a staking pool. There are two types of pooled staking. One where users give up control of their private keys to the pool operator, meaning the operator holds and manages the assets for the delegator. Alternatively, some staking pools function on a non-custodial basis, enabling users to maintain control over their private keys. In this scenario, users delegate their staking rights while keeping custody of their assets.

In the case of delegated staking with ETH, the ETH belonging to the user is transferred to a validator account with validator and withdrawal key pairs, but only the validator private key is generally entrusted to the StaaS provider, while the owner of the ETH that have staked retains the withdrawal private key. Therefore the user (delegator) has control over the means of access to crypto-assets and not a third party.

Regulatory overview of custodial solutions for delegated staking

Custodial services that facilitate delegated staking may involve a contractual relationship between the service provider and the Delegator. Delegators will transfer their assets to the custody provider who will manage the staking on their behalf. In these cases, users do not retain control of their private keys.

This relationship is governed by MICA, making it subject not only to the specific requirements of the service but also to prudential and liability rules that provide extra protection for users in cases of misconduct by the service provider, or of external criminal behaviors.

Article 67 of MICA lays down prudential safeguards that CASPs must put in place at all times for the provision of crypto-assets services- which encapsulates custody and administration of crypto-assets. Paragraphs 4 and 6 state:

> *''4. The prudential safeguards referred to in paragraph 1 shall take any of the following forms or a combination thereof:*
>
> *-(b) an **insurance policy** covering the territories of the Union where crypto-asset services are provided or a comparable guarantee.*
>
> *(...)*
>
> *6. The insurance policy referred to in paragraph 4, point (b), shall include coverage **against the risk of all of the following**:*
>
> *(e) **losses arising from business disruption or system failures;***

> *(f) where applicable to the business model,* ***gross negligence in the safeguarding of clients' crypto-assets and funds;***
>
> *(g)* ***liability*** *of the crypto-asset service providers* ***towards clients*** *pursuant to Article 75(8)"*

Article 75 (8) provides:

> *"****Crypto-asset service providers providing custody and administration of crypto-assets*** *on behalf of clients* ***shall be liable*** *to their clients* ***for the loss*** *of any crypto-assets* ***or of the means of access*** *to the crypto-assets* ***as a result of an incident that is attributable to them.*** *The liability of the crypto-asset service provider shall be capped at the market value of the crypto-asset that was lost, at the time the loss occurred."*

Article 67 ensures that clients are covered for losses resulting from unforeseen events that disrupt the normal operations of the CASP, such as technical failures, cyberattacks, or other incidents that could hinder access to their crypto-assets. The clause also covers any gross negligence in CASP's duty to protect clients' assets. In addition, if a CASP fails to implement adequate security measures or acts recklessly in managing client funds, the insurance policy must cover the resulting losses.

In parallel, Article 75(8) further reinforces the accountability of CASPs by explicitly stating that they are liable for losses incurred by clients due to incidents that can be traced back to the CASP's actions. This provision is critical in establishing a clear legal framework for liability, ensuring that clients have recourse in the event of asset loss.

Additionally, Article 71 provides for complaints handling requirements. This process allows customers to lodge complaints, providing for a fair and efficient resolution of complaints with the CASP before engaging in any dispute resolution or ultimately, judiciary action.

In summary, the prudential safeguards outlined in Article 67, along with the liability provisions in Article 75(8), create a comprehensive regulatory framework that enhances the security of the provision of crypto-asset services. By mandating insurance coverage and establishing clear liability standards, MICA protects clients' interests and fosters a more secure and trustworthy environment, ultimately benefiting all participants involved. This regulatory approach not only mitigates risks for clients but also encourages CASPs to adopt best practices in asset management and security.

In practice, this means that if the custodian providing staking services fails to uphold their responsibilities, they can be held liable for any resulting damages in cases of misconduct related to asset custody. Additionally, users are yet afforded protection against the criminal actions of external third parties, ensuring that their interests are protected in the event of fraudulent activities or other malicious behaviors.

In addition to the requirements mandated by MiCA, there are some market practices that players are implementing to offer additional protection and confidence to the user. For example, they may offer insurance to protect themselves and their stakeholders from certain risks.

C) Applicable regulatory standards from a technological point of view

As we have seen, in the context of staking, cybersecurity is a paramount component of the custody and administration of crypto-assets due to the digital nature of these services.

Yet, Services that offer staking solutions may also be subject to cyber-security standards under 3 important European legislations: 1) The Digital Operational Resilience Act; 2) The Cyber-Resilience Act; 3) Product Liability Directive.

The Digital Operational Resilience Act (DORA)

DORA aims to enhance the operational resilience of financial entities, including CASPs, by establishing uniform requirements for the security of networks and information systems supporting their business processes.

The key components of DORA relevant to StaaS include a risk management framework aimed to promptly and efficiently identify, assess, and mitigate risks associated with their digital operations. This includes specific provisions for cybersecurity risks that could impact the integrity and availability of staking services.

Also embeds incident reporting obligations, under which CASPs must report significant operational incidents, including cybersecurity breaches, to relevant authorities within a specified timeframe. This requirement ensures that stakeholders are informed about potential risks and can take necessary actions to protect their assets.

DORA also requires CASPs to develop business continuity and recovery plans and to set up regular testing and resilience assessments.

Although this is already a natural and extended market practice, this proactive approach helps identify vulnerabilities in staking services and strengthens defenses against potential cyber threats.

Cyber-Resilience Act (CRA)

The Regulation lays down cybersecurity requirements for economic operators in relation to making available "products with digital elements" on the EU market. Software or hardware are considered products with digital elements under the regulation, and their manufacturers are subject to the established cybersecurity requirements, where made available in the course of a commercial activity.

The CRA defines manufacturers as persons who develop or manufacture the products and market them under their name or trademark, whether for payment, monetization, or free of charge. Therefore, CASPs could be considered manufacturers of tokens, protocols, Smart Contracts or CASPs apps, crypto assets wallets, and other types of Web3 products when making them available under their name/trademark.

Essentially, under CRA, manufacturers shall ensure that the product has been designed, developed, and produced in accordance with the essential cyber-security quality checks set out in the Regulation, and shall update the product design to ensure the appropriate level of security. The CRA includes procedures for detecting, responding to, and recovering from cyberattacks that could cover staking services.

Product Liability Directive (PLD)

The Product Liability Directive addresses the liability of producers for damages caused by defective products. The PLD may hold CASPs liable for damages resulting from defective products where required cyber-security quality has not been ensured. This creates a strong incentive for CASPs to prioritize cybersecurity measures to protect user assets. The Directive aims to protect consumers by ensuring that they have recourse in the event of losses due to defective products or services.

→ Custody in staking

MiCA does not contain specific provisions in relation to staking and it is not subject to specific licensing requirements however it has been confirmed that staking is permissible activity under MiCA. Where services are provided in combination with another regulated activity eg custody, those staking services would need to meet MiCA requirements.

However, Direct staking, staking via a non-custodial service provider (eg StaaS infrastructure service provider) or by Defi solutions, does not qualify as a custody service for crypto-assets as the user retains ownership of their assets / private keys and/ or crypto asset services "*provided in a fully decentralised manner without any intermediary*" fall outside of MiCA scope. Since transfers are automated, decentralized, and do not involve any discretion on the part of the protocol as to the use of the assets as collateral, they cannot be considered held on behalf of third parties. Smart contracts automate the entire process of staking, validation, and asset return. After a validator initiates staking, the protocol automatically manages asset locking and unlocking without any party intervention.

Self-custodial staking models do not result in custody of the user's private keys/assets - the withdrawal keys, which control the address and is eligible to receive the original stake and any accrued rewards upon a withdrawal, are controlled on the self-hosted wallet. In contrast, staking infrastructure service providers have the validator private key for signing blocks which don't enable you to move/control or transfer in title of the delegated assets, it just enables you to run the validator / validates transactions. It is misconception is to conflate control of keys associated with the running of a validator with custody/control of keys for delegated assets (including withdrawal keys).

However, the technological tools used to perform staking may still be subject to the cybersecurity requirements and liability standards laid down in the Cyber-Resilience Act and the Product Liability Directive.

B. Qualification of Liquid Staking Tokens

What is liquid staking?

Before we provide legal considerations on Liquid Staken Tokens, first, it is important to dive into what is Liquid staking.

Liquid staking is a process that allows crypto-assets holders to secure the network and receive staking rewards without sacrificing the liquidity of their assets. By depositing their crypto-assets into a liquid staking protocol, holders receive Liquid Staking Tokens (LSTs) that can be traded or used in other decentralized finance applications.

These tokens represent the staked assets and can be freely traded or utilized in decentralized finance (DeFi) applications, thereby, enabling users to earn staking rewards without relinquishing access to their underlying assets. LSTs are issued by liquid staking protocols as a representation of the underlying staked assets that are deposited by users. When a user stakes their crypto-assets through a liquid staking protocol, they receive LSTs. This ensures that the value of the LSTs is directly correlated to the value of the staked assets, providing users with a secure and liquid alternative to traditional staking.

User perspective on the Liquid Staking process

First, the user selects a liquid staking protocol that supports the chosen crypto-asset and initiates the staking process by depositing the tokens into the protocol's smart contract.

Upon deposit, the liquid staking protocol issues LSTs to the user. These tokens represent the user's stake in the protocol and are a “receipt” or “certificate” to the underlying staked assets. For example, if a user stakes 10 ETH, they might receive 10 LSTs that represent their claim to that staked ETH.

As the staked assets generate rewards (native tokens of the blockchain) once the validation process is successfully completed, these rewards are typically distributed to the liquid staking protocol. The protocol then allocates a portion of these rewards to the holders of LSTs. The mechanism for distributing rewards can vary by protocol, but it often involves either a “direct distribution” or a mechanism of value appreciation.

In a direct distribution model, users will receive additional tokens directly into their wallets based on the amount of LSTs they hold. However, the value of the LSTs may increase over time as the protocol accumulates rewards, reflecting the increased value of the underlying staked assets. The value appreciation then occurs when the protocol adjusts the value of LSTs to account for the rewards earned.

When a user holds LSTs but has not yet claimed a redemption, the underlying crypto-assets remain staked in the liquid staking protocol. The staked assets continue to earn rewards as long as they are in the staking contract as they continue to actively participate in the staking process. It is worth pointing out that users are entitled to un-stake their deposit asset and redeem their LST at all times.

The redemption process may require a waiting period depending on the protocol's rules. The length varies by network and can range from a few days to several weeks. For example, in Ethereum is set to be around 7 days.

This so-called "cooldown period" helps to maintain the security and stability of the PoS network as it prevents users from rapidly entering and exiting staking, which could lead to instability in the network's consensus mechanism. This period allows the network to finalize any pending transactions, without disrupting ongoing operations.

To initiate the process, first, the user submits a request to redeem their LSTs through the liquid staking protocol's interface. Technically, this request is usually performed via a smart contract. During this period, the user cannot trade or transfer these LSTs until the redemption process is complete. They can track the status of their request through the protocol's interface.

The protocol will then initiate the unstaking of the corresponding amount of the underlying crypto-assets. This process may involve a cooldown period, during which the assets are still earning rewards. Once the unstaking period is over, the user will receive their original staked assets back in their wallet plus the rewards earned during the staking period.

Burning LST after redemption

In many liquid staking protocols, the LSTs that were redeemed are burned. This means that the tokens are permanently removed from circulation, effectively reducing the total supply of LSTs. This process is transparent and verifiable on the blockchain. In addition, burning LSTs helps manage the total supply of tokens in circulation, ensuring that the total number of LSTs reflects the actual amount of staked assets in the protocol.

The burning process is usually executed through a smart contract that automatically handles the transfer of LSTs to a burn address upon redemption. This is typically done by sending the tokens to a wallet address that is inaccessible or has no private key, effectively making them irretrievable.

Once LSTs are burned, they cannot be reused or recovered. The act of burning is irreversible, as the tokens are permanently destroyed and cannot be retrieved by any party, including the original owner. Either cannot be stolen because they are sent to an address that is effectively inaccessible since there is no private key associated with the burn address.

Ownership of traded LST

Importantly, trading LSTs does not impact the underlying staked assets. The assets remain in the staking contract, and the staking rewards continue to accrue as long as the assets are staked.

When a user trades their LSTs, the new owner of those tokens assumes the rights to any future rewards associated with those LSTs. The original staker no longer has any claim to the rewards once the LSTs are sold. The underlying crypto-assets that were staked are not burned or affected by the trading of LSTs. The assets remain staked in the protocol, and the staking rewards continue to accumulate based on the total amount staked. In addition, the protocol typically tracks the ownership of LSTs to ensure that rewards are distributed to the correct holders.

Qualification of LST

Article 3 (5) of MiCA defines crypto-assets as "*a digital representation of a value or of a right that is able to be transferred and stored electronically using distributed ledger technology or similar technology*".

From the perspective of MiCA's definition, LSTs can indeed be seen as a digital representation of value or rights. LSTs perform as a "receipt" or proof of the staked tokens, allowing users to retain liquidity while their assets are locked in the staking process. They also confer the right to redeem the original staked crypto-assets.

Thus, LSTs are mere tradable certificates of ownership that mirror the value of the deposited (staked) assets.

It is important to bear in mind that LTSs are typically minted and distributed through decentralized protocols rather than by centralized entities. LTSs are often generated through smart contracts on liquid staking protocols. Those protocols operate under a decentralized governance model, where decisions regarding the issuance and management of LTSs are made collectively by token holders.

Yet and importantly, LST cannot be categorized neatly into the categories of crypto-assets listed in MICA given there is no offer to the public. LSTs are minted and transferred directly to the user who has staked the crypto-assets within a specific platform or protocol. This means that the issuance of LTSs is limited to participants of that protocol rather than being made available to the general public. In addition, LTSs are not marketed or promoted in the manner of categorized MICA crypto-assets. This indicated that there is no intention to make a public offer.

Furthermore, any tentative to categorize them with assets reference tokens (ARTs) will fail to recognize that LSTs are intrinsically not issued for the purpose of providing a stabilized value to the token. They do not qualify as ARTs, as are not intended to maintain stable value by reference to underlying collateral. Instead, they confer the possibility to the user to keep making use and enjoy the economic benefits of the staked tokens, as well as a proof of redemption rights in relation to the staked tokens.

They shall not be deemed as derivatives either. LSTs do not create contractual options like derivatives do, they are simply tokens that represent staked assets. LSTs do not represent a contract or pre-setted conditions to buy or sell an asset in the future; instead, they are a direct representation of current ownership of the staked assets and the associated rewards. Indeed, LSTs are not primarily designed for speculation on the price movements of an underlying asset. While their market price may fluctuate, the primary purpose of LSTs is to provide liquidity and access to staking rewards, rather than to serve as a speculative instrument.

5. Policy recommendations

1) **Staking should be recognized as a technological activity and not a financial service.**
2) **Policymakers should differentiate between custody services and the technical process of staking. Non-custodial services should be excluded from regulatory oversight.**
3) **It is paramount not to conflate risks posed by primary activities (eg custody) with ancillary staking services.**
4) **A bespoke staking framework is not required. We encourage policymakers to look at existing requirements and how these can be leveraged to mitigate risks posed as appropriate. Existing regulatory standards already applying to the ecosystem must be taken into consideration to avoid over-regulation, disproportionality, and hurdles imposition which would slow down the nascence of innovative projects and could harm the competitiveness of the market.**