A Comparative Analysis of Staking Protocols in Blockchain Networks

Dominic Wallis Ph.d, Christian Koch M.A.

Abstract

This paper provides a brief comparison of various staking protocols across different blockchain networks and an assessment of each against an initial understanding of system requirements identified by Orcfax, which seeks to ascertain whether an existing solution, as a drop in solution for Orcfax, adequately meets its needs. However, it was found that no single staking protocol from the sample set fully meets all requirements outlined in the Orcfax Staking Protocol Requirements; each protocol was found to have its strengths, but they collectively fall short of the preliminary system requirements in one or more critical areas.

While there are a multitude of staking protocols in operation, this paper has analyzed a limited sample which is meant to be representative; included in this assessment are the staking protocols utilized by: Algorand, Avalanche, Bitcoin Lightning, Cardano, Cosmos, and Ethereum. Each protocol's mechanism for staking, rewards, and penalties are examined in light of Orcfax priorities for network security, equitable participation, and long term decentralization in order to better understand each protocol's features and the implications of use for Orcfax participants.

1. Introduction

What is staking

In the context of blockchains and crypto currency, the original use of the term "staking" is credited to Peercoin. Peercoin introduced a Proof of stake consensus protocol as an alternative to Bitcoin's proof of work. The protocol requires those participating in consensus to 'lock up' their native currency PPC. By doing so, the likelihood of a participant having the ability to mint the next block is determined by the relative 'coin age' of their stake. Coin age being determined by the length of time those assets had been locked.

The authors of the protocol claim that this mechanism is too expensive to be abused for an attackers financial advantage.

Since Peercoin's inception, the term 'staking' has been used by many different protocols to describe mechanisms in their own protocol that share some characteristics with that of Peercoin. However, there is significant divergence in what these mechanisms are to the extent that they have overlap. For example, staking on Cardano refers to participants using their funds to aid the health of the network (like Peercoin), but it is delegated and not locked (unlike Peercoin). In contrast, staking on Ethereum 2.0 is done only by those actively participating in consensus, and this stake is locked and slashable.

In further contrast, the term is also employed when only referring to assets being 'locked', and not always when related to participation.

source

What does Orcfax mean by staking?

While the previous section illustrates how the term "staking" has been used inconsistently after its inception, Orcfax takes staking to mean:

The 'financial' incentive structure aimed at encouraging good and/or discouraging bad behaviour of the participants of a decentralised network. The ultimate goal of staking being to ensure the network remains active in a sustainable way.

What is Orcfax and what is its need for staking?

Orcfax is an aspiring decentralized oracle protocol built on top of Cardano. As Orcfax prepares to transition to a fully decentralized service provider, it will begin by distributing oracle tasks across a network of node operators. The collection of these participants providing oracle services form a decentralized network. These participants must produce 'statements' for those whose protocols require the consumption of oracle data (i.e. consumers).

An important feature of this network will be the use of staking. Orcfax wishes to construct a staking mechanism that aids its long term health, and inspires confidence in their consumers that statements will be accurately and promptly produced now and into the future.

By nature of being an oracle, much of the Orcfax protocol does not and cannot operate within the context of a blockchain. The staking mechanism implemented must reflect this.

Furthermore, the participants of the service provision must be holders of an NFT token series on Cardano, the Orcfax Validator Licenses. There are 100 of these licenses.

Orcfax will require participants to maintain a specified stake and be holders of one Orcfax Validator License NFT, of which there are 100, in order to prove their "skin in the game" and to participate in oracle related tasks. Should operators perform as desired, they will be rewarded proportionate to their performance. If operators perform in undesirable ways, some staking protocols utilize "slashing" as a punishment whereby some, or all, of the staked assets may be removed from the participant. However, care must be taken; the wrong incentive structure may either: cause a race to the top, where rewards only go to a few participants which eventually leads to centralization; or, cause a race to the bottom, where participants are rewarded even if they are poor service providers. Both of which are bad for the long term health of the service.

As the integration of any staking mechanism will dramatically affect how operators participate within the network, it is imperative that Orcfax understands the implications of staking mechanism design choices. As such, this paper seeks to understand the current state of staking protocols across blockchain networks and whether any may be of use to Orcfax. This paper uses a qualitative research method and has primarily used the publicly available documentation and publications provided by each protocol.

2. Context

In order to develop a critical framework by which staking mechanism could be compared, Orcfax combined a preliminary vision for the mechanism, a draft set of system requirements, and participant requirements. The combination of these serve the sole purpose of providing Orcfax with a foundation and structure by which the sample set could be assessed.

Additionally, each staking mechanism is examined in light of Orcfax priorities for network security, the degree of or opportunity for equitable participation, and how each might contribute to the long term decentralization goals of the Orcfax network.

The Orcfax staking protocol should operate within a decentralized service framework, where participants, both competent and potentially malicious, must work

together to provide reliable service. The system's design must seek to emphasize the incentivization of good behavior and penalization of bad actions through its staking mechanism.

2.1 Key components of the staking mechanism

1. Decentralized Service: The protocol relies on a network of autonomous participants with a shared goal, requiring mechanisms to reward good service and discourage malfeasance.
2. Staking Mechanism:
    - Slashing: Participants must lock certain assets as stake. If their behavior is deemed malicious, they forfeit a portion or all of their stake.
    - Rewards: Participants earn rewards proportional to their good service, promoting healthy competition without leading to centralization or rewarding poor performance.

2.2 Participant requirements

In order for network operators to participate, Orcfax requires each to stake the following:

- Orcfax Validator License: One of 100 NFTs.
- Minimum stake: 500,000 FACT tokens.

2.3 System components

Orcfax anticipates that regardless of staking protocol, it will consist of the following components:

1. Smart Contracts: Enabling locking, unlocking, rewarding, and slashing of assets.
2. Participant Interface: Allowing actions such as locking and unlocking stake.
3. Decentralized Service Platform: A black box model for assessing participant behavior.
4. Reward and Slashing Management Interface: Facilitating the distribution of rewards and penalties.

2.4 Must Have requirements

Orcfax has identified the following as staking protocol Must haves:

1. A participant can deposit native assets, FT and an NFT, as stake
2. A participant can withdraw their stake, with a cooling-off period
3. A participant with live stake receives rewards for good behaviour
4. A participant with stake is slashed if they behave badly
5. The mechanisms for rewarding and slashing are controlled by a majority
6. Rewards are paid out from a treasury
7. Forfeit funds are paid into the treasury
8. Forfeit funds are redistributed to an Orcfax wallet
9. The system is efficient when the vast majority of participants are honest and while most participants are competent
10. The system is resistant to abuse by a minority of malicious nodes eg good participants are protected from slashing
11. The network must bee able to accommodate ~100 nodes.

In addition to this initial draft of system requirements, each staking mechanism assessed within this paper will be evaluated against Orcfax priorities for:

- Security: to what degree is it apparent that the design choices for each staking mechanism impact the overall security of the network?
- Participation: to what degree does the staking mechanism provide opportunities for equitable participation within the network?
- Decentralization: Given the previous two, to what degree do choices influencing network security and participation have on the degree of decentralization or any risks towards centralization of the network?

3. Overview of staking Protocols

While this paper does not cover the breadth of staking protocols being used across the multitude of blockchain networks, care was taken to select protocols which together are representative of the different methods for implementing staking. The following protocols are discussed in alphabetical order: Algorand, Avalanche, Bitcoin Lightning, Cardano, Cosmos, and Ethereum.

These protocols have been assessed against the requirements outlined in the "Orcfax staking protocol requirements" and in light of Orcfax priorities for network security, equitable participation, and long term goals for decentralization.

3.1 Algorand

Algorand is a proof-of-stake blockchain that requires users to hold its native token, Algo, to participate within the network. The minimum stake to participate is effectively 1 Algo. This staking mechanism is notable in that it allows users to retain control of their staked Algo even while participating in consensus. However, participation does not yield rewards currently, which raises concerns about user incentives to run nodes. In addition to the absence of rewards, there are not yet any penalties for bad behavior.

> Participation in consensus currently does not affect the proportion of participation rewards an account receives. Participation rewards are based on the amount of stake an account has, irrespective of whether the account is marked online or offline. Furthermore, currently there are no participation rewards on MainNet.

source

While there is no minimum threshold, the probability in actively participating is proportional to the stake, which is not locked and is not slashable.

The protocol has some limited support for rewards. However it is currently not utilised - rewards are effectively set to 0.

The architects of Algorand have raised concerns about the levels of participation in consensus. Moreover, there is a suggestion that lack of rewards contributes to the problem. The following quote is taken from *Algorand Consensus Incentivisation: An Algorand foundation discussion paper*(Woods, Treccani, Jannotti, 2023).

> Algorand's original thesis contended, a priori, that a sufficient number of end-users would naturally be incentivised to run a node and contribute to online stake, motivated by the desire to secure their own funds, and as a corollary the network. However, a posteriori, it has been observed that as a consequence of the cost to run a participation node with high uptime, and indeed the technical expertise required to both instantiate and maintain a node, a critical mass of end-user contribution has not been reached.

source

Given the above, an assessment of Algorand documentation against Orcfax system requirements results in the following:

1. **Security:** Algorand employs a consensus mechanism with the aim to enhance network security without compromising decentralization, however it does not currently employ an incentive structure to promote goof behavior or disincentives to discourage bad behavior; our limited research did not reveal whether this posed a potential security risk for the network.
2. **Participation:** The lack of rewards for participation on the mainnet may result in low engagement. While the staking mechanism allows users to maintain control over their funds during staking, the absence of incentives may hinder broader participation.
3. **Decentralization:** Algorand's model promotes decentralization by allowing all holders of Algo to participate in consensus. However, the technical complexity and costs associated with maintaining high uptime for nodes without an incentive to do so may discourage potential validators, leading to centralization risks.

Taken together, the staking protocol used by Alogrand as a drop in solution for Orcfax partially meets the requirements, particularly in security and decentralization, but falls short in providing effective incentives for participation, which is crucial for a robust staking ecosystem. An additional strength of the protocol is its emphasis on accessibility; Algorand allows any user to participate in securing the network by allowing any holder of Algo (of any amount) to participate and users maintain control of their assets at all times, making it user-friendly for those in diverse financial situations and for those who prefer non-custodial solutions.

However, the absence of participation rewards is assessed as a design weakness and one which if incorporated into an Orcfax solution could lead to low user motivation to run participation nodes. This is a significant gap in meeting the requirement for robust incentives. Additionally, the lack of penalties for bad behavior is assessed as a risk which may reduce the overall security of the network as there is no deterrent against malicious activity.

3.2 Avalanche

Avalanche is a PoS blockchain which employs a validation mechanism where participants must stake AVAX tokens in order to validate transactions. A minimum stake of 2,000 AVAX is required to participate on mainnet while 1 AVAX is required to participate on their testnet (Fuji); when it comes to participation, validators are sampled for consensus based on the proportion of their stake, which means that participants may be incentivized to increase their stake.

While the minimum stake could prove a challenge to entry, the network justifies it as a security feature.

"To resist sybil attacks, a decentralized network must require that network influence is paid with a scarce resource. This makes it infeasibly expensive for an attacker to gain enough influence over the network to compromise its security."

source

Avalanche also enables holders to delegate their AVAX to validators; a validator's influence therefore is increased not only by their own stake above the minimum, but may be increased through delegation up to a maximum of 3 million AVAX. This ability to delegate to validators enables holders to assist in securing the network, receive rewards for their delegations, and do so without the overhead of being their own validator. However, delegators are required to hold a minimum of 25 AVAX on mainnet in order to delegate.

source

Participation as a validator is incentivized by rewarding uptime. Validators are eligible for rewards for their efforts securing the network, which is measured through the total time their node is active and participating within the network. Through random sampling executed by their peers, a validator's node must be found to be active or responsive more than 80% of any given validation period.

source

With that said, there are no penalties or slashing for bad behavior committed by validators. The only risk that participants face is becoming ineligible for rewards by failing to meet specified parameters.

Given the above, an assessment of the Avalanche documentation against Orcfax system requirements results in the following:

1. **Security:** Avalanche's high minimum stake threshold for participation and incentive structure through random sampling of validator node uptime promotes security of the network and may enhance resilience against attacks. And while this aspect of the model aligns well with the Orcfax requirement for a secure staking environment, the absence of penalties leaves something to be desired.
2. **Participation:** Broad participation as a validator may be limited by a minimum stake which could be perceived as a high cost to entry; Avalanche may have tempered this criticism by enabling the option for delegation, which thereby allows users with smaller stakes to engage without needing to run a full node.
3. **Decentralization:** The difference between the minimum stake for validators (2,000 AVAX), the maximum combined stake and delegation (2m AVAX), and weighted validator influence mechanic may pose centralization risks if reaching the maximum is competitive and results in a few validators holding increased influence over the network. Conversely, the delegation feature may help to mitigate this risk by allowing a more distributed participation model.

Taken together, the staking protocol used by Avalanche as a drop in solution for Orcfax partially meets the requirements regarding security and incentives for participation; the simplification of incentivizing uptime conveys a clear reward structure based on the amount staked, which may effectively motivating users to participate actively. The lack of penalties or slashing is notable. While limiting the scope of the incentive structure to whether a node is eligible or ineligible may not sufficiently deter negligence or bad behavior.

Additionally, security as a strength appears to come at the cost of participation; the minimum stake to participate in the network may prevent broad participation from holders, although it is acknowledged that enabling delegation may work to address this shortcoming. With that said, care may need to be taken to deter potential centralization risks.

3.3 Bitcoin Lightning

As a layer-2 solution on Bitcoin, the Lightning Network is comprised of bidirectional payment channels between participants which facilitate off-chain transactions. In this system Bitcoin is locked in order to open an LN payment channel. LN, in its original conception, the network introduced an incentive structure whereby users locked funds as stake in the sense that if one participant of a channel were to behave badly in a provable way, the other participant of the channel would be able to take the locked stake.

However, more recent iterations (e.g. eltoo aka LN-symmetry) have opted to remove this penalty centric incentive structure on the grounds that it complicates the design, and can result in unintentional penalties for participants.

source

Given the above, an assessment of the Bitcoin Lightning paper against Orcfax system requirements results in the following:

1. **Security:** The Lightning Network's design inherently deters malicious behavior through the risk of losing locked funds. However, the current penalty system may require careful enforcement to maintain trust among participants.
2. **Participation:** The LN's unique model allows for rapid transactions between participants, however, the complexity of managing channels and the potential for penalties could deter participation.
3. **Decentralization:** As a layer two solution, the LN depends on the underlying network for security. This dependency can lead to varying levels of

decentralization.

Taken together, the staking protocol used by Bitcoin lighting as a drop in solution for Orcfax partially meets the requirements. While it offers a secure and innovative model for transaction processing which inherently deters malicious behavior through the risk of lost stake and thereby creates a strong disincentive for dishonest actions within payment channels, the complexities and potential penalties involved may limit broader participation. Additionally, while efforts have been made to create iterations which remove penalties, this may undermine the incentive for participants to maintain honest behavior, which is a critical requirement for staking protocols.

3.4 Cardano

Cardano is another prominent proof-of-stake blockchain utilizing its native token, ADA. Stake pool operators (SPOs) are block producers and are required to stake 500 ADA in order to operate their nodes. SPO's are incentivized to participate through block producing rewards, and there are no penalties or slashing for bad behavior.

Holders have the ability to delegate their ADA to these SPOs and may be rewarded by doing so; the ADA which these users delegate is not locked and is not slashable. The likelihood of any given node producing a block is, in part, determined by the amount of stake and volume of delegation attributed to it. A block producing node receives rewards for their services in securing the network. Generally some of the awards received by the SPO's are ultimately shared with those who delegated to the pool, but each SPO can adjust whether, and to what degree, this is done.

Given the above, an assessment of the Cardano documentation against Orcfax system requirements results in the following:

1. **Security:** The design of Cardano's Ouroboros consensus algorithm incentivizes SPOs to actively participate in block production. However, the absence of slashing penalties is noteworthy as there does not appear to be an effective way of disincentivizing malicious behavior.
2. **Participation:** The stake and delegation model encourages increased user participation by allowing non-SPOs delegators to earn rewards without needing technical expertise. The competitive nature of stake pools promotes active engagement, which meets the Orcfax requirement for incentivized participation.
3. **Decentralization:** By setting the minimum stake for SPO's relatively low and by allowing other holders to leverage their ADA through its delegation system Cardano prioritizes decentralization of network participation through user choices in terms of where they delegate.

Taken together, the staking protocol used by Cardano as a drop in solution for Orcfax effectively meets the requirements across incentives, and decentralization, positioning itself as a strong contender in the staking landscape. The ability for users to delegate without locking funds encourages broad participation while the competitive nature of those delegations may influence SPO performance in order to maintain them.

3.5 Cosmos

Cosmos facilitates a network of interconnected blockchains, utilizing the PoS Tendermint consensus mechanism and its native currency ATOM; with that said, the current fork that is used is "CometBFT", which notably is a BFT based algorithm.

Any holder of ATOM may either declare their intention of becoming a Validators, or choose to delegate their ATOM to one of these validators in order to earn rewards. For those seeking to become validators, the total number of active validators on the network is limited. At the time of this writing, the total number of validators is limited to 180, but this number can be adjusted through governance protocols; in order to secure the ability to operate as a validator and participate in the network by committing blocks, validators must compete for the highest volume of total stake & delegations; those with volumes in the top 180 are then designated validators.

source

Notably, the stake and delegations are locked and can be slashed. The following is an excerpt from their whitepaper:

> Validators in Cosmos have a similar role to Bitcoin miners, but instead use cryptographic signatures to vote. Validators ... are responsible for committing blocks. Non-validators can delegate their staking tokens (called "atoms") to any validator to earn a portion of block fees and atom rewards, but they incur the risk of getting punished (slashed) if the delegate validator gets hacked or violates the protocol.

source

This is similar to Cardano, in that users can delegate to dedicated validators, and then take a share of rewards. However, a key distinction in Cosmos is that (non-validator) users may also *lose* their stake if the validator behaves badly. This dual structure incentivizes users to choose reliable validators to mitigate their risk of slashing, and the competitive nature of delegation, in order for validators to maintain their privileges, may work to further incentivize good behavior on the part of the validator.

Cosmos's focus on interchain interoperability appears to necessitate a focus on bridges. Whereby Participants validating txs across a bridge are *bridge-zone validators*. However, the details of this role are not fleshed out in the original whitepaper; the whitepaper says only that validators should stake collateral to be forfeit in the event of bad behavior in order to disincentivize it.

Given the above, an assessment of Cosmos documentation against Orcfax system requirements results in the following:

1. **Security:** The high minimum stake threshold for participation, that inevitably occurs through the competitive nature of maintaining the role of a validator, combined with the Cosmos incentive structure promotes security of the network and may enhance resilience against attacks. This aspect of the model aligns well with the Orcfax requirement for a secure staking environment and includes slashing as a penalty for bad behavior.
2. **Participation:** The absence of an explicit minimum stake threshold for validators may have broadened participation early on, but the competitive nature of maintaining a large total volume of both stake and delegations my create barriers for entry as the network grows. However, the incentives for holders to delegate their ATOM and receive rewards allows for multiple avenues for users to participate in securing the network. It is unclear whether the risks related to slashing deter broader participation in delegation.
3. **Decentralization:** Cosmos promotes decentralization through its multi-chain architecture, allowing various independent blockchains to interact. However, the competitive nature of securing total stake and delegation volume in order to provide collateral for cross-chain transactions could result in a centralization risk if few participants ran many nodes. Possibly as a response to this criticism, Cosmos does have the ability to increase the total number of validators through governance actions.

Taken together, the staking protocol used by Cosmos as a drop in solution for Orcfax meets several requirements but faces challenges related to its incentive structure and potential centralization risks. While Orcfax has identified slashing as a requirement in order to disincentivize malicious behavior, we had not considered slashing non-validator delegations. Additionally, the absence of a maximum stake and delegation volume combined with the need for validators to compete in securing delegation volumes, while potentially adding to an incentive structure, may provide a centralization risk. It would be essential for Orcfax to address these issues prior to implementation in order to align with its requirements and to strengthen its own network.

3.6 Ethereum

Ethereum is the largest blockchain based on total value locked (TVL) and has recently transitioned away from a proof-of-work consensus mechanism to its current PoS mechanism. Those looking to participate in securing the network must stake a minimum of 32 ETH to become validators; And while non-validator holders do not have the ability to delegate to validators for a share in rewards, as some of the other chains in this paper allow, participants have multiple methods by which they may operate validator nodes:

- as an independent (i.e. Home staking)
- by leveraging cloud compute (i.e. Staking as a Service)
- by pooling (which allows multiple holders to mutually participate)
- or by staking through a CEX (i.e. Centralized Exchange)

source

And each of these methods varies in terms of expected rewards for the participant.

Ethereum has deployed an incentive structure in order to reward participants for helping in securing the network. Rewards are given for actions that help the network reach consensus. Validators may receive rewards for running software that properly batches transactions into new blocks, and when they check the work of other validators.

source

The Ethereum FAQ page suggests that because these tasks are constantly being executed, validators are essentially incentivized for their uptime and that validators may expect their services to be net profitable so long as the validator's uptime is greater than 50%.

source

But the Ethereum incentive structure isn't limited to just incentives, the staking protocol also utilizes penalties or slashing for bad behavior. Ethereum defines slashing as follows:

> Slashing has two purposes: (1) to make it prohibitively expensive to attack the network, and (2) to stop validators from being lazy by checking that they actually perform their duties. If you're slashed because you've acted in a provably destructive manner, a portion of your stake will be destroyed.

source

Accordingly, being offline for brief periods of time results in small inactivity penalties to accrue against validators, however, validators may annul these penalties through uptime. With that said, Ethereum adjusts these penalties based on how many validators are operating, with more severe penalties being executed when large number sof validators are down at the same time.

It's important to note that the minimum amount that is slashed is 1 ETH and that validators may not participate so long as their stake is below the required 32 ETH.

Given the above, an assessment of the Ethereum documentation against Orcfax system requirements results in the following:

1. **Security:** Ethereum's transition to a proof-of-stake model enhances security through its rigorous validator requirements and slashing penalties for malicious behavior. This approach aligns well with the need for a secure staking protocol.
2. **Participation:** The varied staking options—solo, pooled, and staking-as-a-service—provide flexibility for users, catering to different technical expertise levels. However, the requirement for 32 ETH to become a solo validator may limit participation for smaller holders, creating a barrier to entry.
3. **Decentralization:** Ethereum's reliance on slashing penalties aims to promote accountability among validators. However, the complexity of its staking mechanism could inadvertently favor larger participants, posing risks to decentralization.

Taken together, the staking protocol used by Ethereum as a drop in solution for Orcfax generally meets the requirements, particularly in security and participation incentives, but falls short when it comes to methods for participation, barriers to entry, and the resulting potential centralization; the requirement of 32 ETH, at its current pricing, may exclude smaller holders from direct participation, although pooled staking options exist. Regarding the incentive structure, the ability for validators to both earn rewards for good behavior and face slashing penalties for malicious actions or prolonged inactivity, making it a high-stakes environment, aligns with Orcfax requirements.

4. Comparative Analysis

4.1 Incentives for Good Behavior

All of the reviewed protocols aside from Algorand incentivize active participation through rewards. In contrast, Algorand's lack of participation rewards raises concerns about user engagement. Cardano and Bitcoin Lightning provide unique approaches to user incentives without penalties, but the lack of disincentive for malicious behavior could be seen as a network security risk.

4.2 Penalties for Malicious Behavior

Owing to the mixed use of penalties or a slashing mechanism in the staking mechanisms reviewed, it is not clear whether the presence or absence of slashing significantly impacts network security. Ethereum and Cosmos employ slashing to deter malicious actions, whereas Avalanche, Algorand, and cardano have more lenient approaches. Bitcoin Lightning's penalty mechanism depends on channel disputes but could be quite severe; however, this penalty mechanism may evolve in future iterations or be removed entirely.

4.3 User participation and network security

Protocols requiring higher stakes, like Ethereum and Avalanche may encourage good behavior from participants but doing so creates barriers to entry which restricts participation. In contrast, Cardano's low minimum stake and flexible delegation withdrawal policies may attract more participants.

4.4 Findings

This comparative analysis highlights the diverse approaches to staking across different blockchain protocols. Each mechanism's design choices reflect the underlying philosophy of its network, influencing user participation, network security, and overall decentralization. As Orcfax seeks to solve its own need for a staking mechanism, understanding these distinctions and how these design choices affect key design goals will be crucial for network success.

From the staking protocols reviewed, each exhibited unique strengths and weaknesses when measured against the Orcfax Staking Protocol Requirements.

- **Algorand and Avalanche** struggle with incentives and security, limiting their appeal and robustness.
- **Bitcoin Lightning's** complexity and potential removal of penalties may hinder user engagement.
- **Cardano and Cosmos** offer accessible models but vary in terms of risk, particularly regarding slashing.
- **Ethereum's** comprehensive incentive and security structure are commendable, though its high entry barrier remains a concern.

Ultimately, the protocol used by Orcfax must balance accessibility, security, and incentives to meet the evolving needs of staking participants.

5. Conclusion

5.1 Limitations

As stated at the outset, this paper did not attempt to cover the breadth of staking protocols which have been deployed across the numerous blockchain networks active at the time of its writing. Instead, a limited sample was selected which was meant to be representative.

Additionally, the analysis of each of the selected proposals was premised on the documentation and publications readily accessible through each of the blockchain networks' public facing sites.

Further research into the differences, advantages, or downsides to each protocol's staking mechanism could be furthered by the incorporation of alternative research methods such as the following:

1. Empirical Analysis
    - Data Collection: Gather real-time data on staking rewards, participation rates, and network performance for each protocol. This would involve monitoring blockchain explorers and staking analytics platforms.
    - User Surveys: Conduct surveys or interviews with users of different protocols to understand their experiences, challenges, and motivations for participating in staking.
2. Case Studies
    - In-Depth Case Studies: Choose specific projects or use cases within each protocol and analyze their staking dynamics. For example, examining how different stake pools operate in Cardano or how delegation works in Avalanche.
3. Comparative Metrics Development
    - Key Performance Indicators (KPIs): Develop KPIs to quantitatively compare protocols. This could include metrics like average staking rewards, decentralization levels, network uptime, and the impact of slashing on validators.

5.2 Key observations

1. **Incentives**: While protocols like **Cardano** and **Avalanche** offer rewarding systems, they lack robust mechanisms that ensure active participation and engagement, particularly when compared to Ethereum’s strict penalties for negligence.
2. **Security**: Protocols like **Ethereum** provide strong security through slashing, but this comes at the cost of accessibility, as the entry barrier is quite high. Conversely, **Algorand** maintains user control but lacks penalties, which can undermine its security integrity.
3. **Accessibility**: **Avalanche** has a relatively low minimum stake requirement, promoting participation. Conversely, **Ethereum**'s 32 ETH requirement limits access, making it less inclusive.
4. **Risk Management**: Protocols like **Cosmos** introduce slashing risks that can deter participants. **Bitcoin Lightning**'s evolution towards removing penalties could weaken its trustworthiness and security model.

5.3 Closing Thoughts

No single staking protocol from the reviewed list fully meets all the requirements outlined in the Orcfax Staking Protocol Requirements. Each protocol has its strengths and weaknesses, but they collectively fall short of the preliminary system requirements and in one or more critical areas relating to Orcfax priorities.

These results signal some important conclusions. First, that given current understandings of Orcfax network needs, there is no one staking protocol from the sample set which can serve as a drop in solution. Second, that given the discrepancies between Orcfax identified system requirements and the sample set, Orcfax may need to reassess the system requirements developed at the outset of this research.

A revision to system requirements could result in closer alignment with a staking mechanism from the sample set, but this would invariably lead to compromises which could have profound impacts on one or more of the key areas (participation, security, decentralization).