A Comparative Analysis of Consensus Protocols used in Blockchain Networks

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

Abstract

This paper provides a brief comparison of various consensus protocols which were assessed against an initial understanding of consensus requirements and identified validator roles for the decentralized validator network, EchoNet. The purpose being for Orcfax to ascertain whether an existing consensus protocol, as a drop in solution for Orcfax, adequately meets its needs for: high throughput, low latency, fault tolerance, and scalability in a multi-validator environment. Based on the analysis of each consensus protocol and the initial *Must Have* requirements identified by Orcfax, none of the reviewed consensus protocols fully meets the needs of EchoNet. However, the most interesting line for additional inquiry is CometBFT which aligned with several of the core Orcfax requirements for a consensus protocol.

The other consensus protocols examined in this paper were: Hydra, Hydrozoa, Iagon, Lodestar, Midgard, NEM, Raft, Snowball, CometBFT, and VeChainThor. Each was assessed for its efficiency, reliability, scalability, as well as its capacity to support a decentralized, real-time data validation network.

1. Introduction

1.1 What is consensus

In the context of decentralized networks, consensus is the process by which network participants (or validators) reach an agreement on the validity of transactions and the state of the blockchain, without the need for a central authority. Validators are tasked with collectively verifying, approving, and adding new transactions to the blockchain, ensuring the integrity and consistency of the distributed ledger. In PoS networks, consensus relies on validators who are chosen to create new blocks or validate transactions based on their stake.

1.2 What is Orcfax and what is its need for consensus?

Orcfax is an aspiring decentralized oracle on the Cardano blockchain. An oracle is a service that makes information available to the context of code executing within the blockchain. This information is used to determine whether transactions may be deemed valid. Thus those effected by such transactions need to have trust in the oracle system. By its nature the information from an oracle does not come with the guarantees of the blockchain, and so to be useful the oracle must present its own integrity model. This model serves as the justification of why anyone should have confidence the oracle service provider is accurate and reliable.

The data Orcfax provides is arranged into feeds. A feed is generally time series data. For example the ADA/USD exchange rate.

A feed can be thought of as a data pipeline. Data is periodically collected from numerous sources. This data is then subjected to a normalization and aggregation process which outputs a statement belonging to a feed. Each execution of the data pipeline results in a statement.

Currently, the Orcfax network is centralized. This means that at present, the integrity model presented by Orcfax is one of authority; this is where a single centralized authority provides information. This integrity model argues that the combination of legal repercussions, and financial and reputation damage ensures the data provider (Orcfax) is highly motivated to report information accurately and reliably.

An advantage of this approach is that it is relatively simple. A disadvantage of the approach is that it has a single point of corruption and or failure; it relies solely on a single entity to be honest and competent.

The goal of Orcfax since its inception has been to develop towards a decentralized network. The decentralized Orcfax network will be EchoNet, it's participants will be referred to as "Orcfax validators", and these validators will be recognized as such through their ownership of specific assets on the Cardano L1. The integrity model presented through this network will be one of consensus; If a decentralized set of participants are to provide a service such as an oracle service, they must first agree on the information they provide. That is, they must find consensus; this must be accomplished given the assumption that most but not all participants are honest and competent while some participants of the network may be malicious or incompetent.

1.3 The role of the validator

Orcfax Validators will be expected to execute a number of tasks, many of which require consensus. A non-exhaustive list of the tasks that validators must do includes:

- running the existing data collectors and feeds
- ensuring maintenance of existing code base
- ensuring health of data sources / definitions of feeds
- sunsetting and discontinuing underused feeds
- defining and developing new feeds
- ensuring the health of the network (removing bad validators and collectors)
- maintaining optimal remuneration parameters

In the present proposal we are mostly concerned with consensus as it is involved in the running of existing feeds. We hope that the underlying techniques can be directly extended to the other tasks contexts.

The running of the existing collectors and feeds is synonymous with the task of producing statements.

A statement is the interface between Orcfax and its consumers. Consumers are the users of Cardano who are in some way implicated in transactions that consume Orcfax data. For example, an individual who took a collateralized loan via a dApp that integrated Orcfax price feeds, and that was liquidated when exchange rates changed is a consumer.

A statement is *published* on the L1 only if it has a valid signature. Currently a single signer is used. It is envisioned that a FROST-like method would allow the transition from a single signer to a multi-signature (k of n) arrangement. However, Orcfax is not committed to this design and this aspect can be change if it is deemed desirable.

1.4 Securing the network

One aim that Orcfax has for its implementation of consensus is to uphold or secure the health of the network in spite of participants behaving badly: either by incompetence or with malicious intent. For this reason It may be helpful to flesh out *What actions are deemed bad for the health or security of the network?* the

following is a non-exhaustive list demonstrating our current understanding.

1.4.1 An unresponsive participant

We cannot know if this is due to malice, incompetence, or wider network failure beyond what is reasonable to expect is within the participants control.

1.4.2 Collectors reporting spurious information

For example, were it possible for a collector to simply copy and repeat anther collectors' output then they add no additional integrity to the network.

1.4.3 Biased aggregators

Depending on the design, there may be the possibility of an aggregator perform selection bias, ignoring collectors with unfavorable outputs.

1.4.4 Copycat participants

Depending on the design, it maybe possible for a participant to simply copy the results of another participant. This makes the network less robust and reliable.

1.4.5 Half hearted Participants

Suppose there is no check on publishing the data trace then a participant will begin ignoring a stipulation.

1.4.6 Considerations

We don't yet have complete answers to how the design addresses these issues. Such design decisions will likely have a bearing on who is reaching consensus how and over precisely what.

1.5 Consensus requirements

The framing of the requirements is partly based on assumptions on the form of the output.

- The software is, or mimics, a service on a computer.
- Each participant is running an instance of the software.
- State must be communicated between participants.
- If relevant, assume participants can communicate via TCP or UDP based.

Given these, Orcfax has identified the following as a preliminary list of Must Have requirements (parameters outlined below):

1. Participants efficiently communicate their state
2. Participants run validity checks on any data they receive. If appropriate, they will stop communicating with a participant providing bad data.
3. N participants reach consensus.
4. In normal conditions, time < T seconds between an atom being sent from an external source to it being included in consensus by most participants. If finality is not a property of the consensus mechanism, then replace this with an analogous condition (eg high probability etc.).
5. In normal conditions, throughput averaging > V statements per second
6. Impossible to publish a bad statement with K number of malicious nodes
7. Impossible to crash the system with K number of malicious nodes

Parameters:

- N = number of nodes in the network: 100
- K = number of malicious or incompetent nodes: 30
- T = time of delivery: 60s
- V = velocity of statements: 10 tps

2. Overview of consensus protocols

As stated previously, this paper does not begin to cover the breadth of consensus protocols being used across the multitude of blockchain networks. Instead, a sample set of consensus implementations were selected which primarily utilize Proof of Stake (PoS) as this is an Orcfax network requirement, but some alternative consensus mechanisms are also explored.

These protocols have been assessed against a preliminary understanding of Orcfax needs for consensus within EchoNet, the role of Orcfax validators, the identified Must Have requirements, their efficiency, and reliability.

2.1 Hydra

Hydra is an L2 scaling solution designed specifically for the Cardano blockchain. Its purpose is to enhance transaction throughput and reduce latency by creating “Hydra heads,” which are separate, parallelized mini-ledgers that allow for fast and efficient transaction processing independently of the main Cardano blockchain Hydra Protocol, 2023.

Each Hydra head is presented as a scalable, parallel processing environment that maintains strong connections to Cardano’s primary chain, ensuring secure and synchronized state transitions without burdening the main network. The Hydra protocol functions by offloading transaction processing to these Hydra heads. Each Hydra head can be thought of as a decentralized, mini consensus environment where nodes execute transactions and reach consensus independently, but unanimously within the head. These transactions are later aggregated back to the Cardano main chain.

At the time of writing, the largest number of participants demonstrated in a tx is 57. Presumably, this is the most that are able to participate before some tx limit is reached.

2.1.1 Hydra against requirements

Challenges: Hydra as an out of the box solution for Orcfax is immediately ruled out. The reliance of heads on unanimous consent means that one malicious actor could have significant impacts on network reliability and efficacy. However, it might be possible to adapt Hydra by relaxing unanimous consent. Otherwise, Hydra is not too far off meeting the core design requirements; Issues with participation count being limited to 57 might be circumvented for Orcfax's needs. It may also be possible that hydra brings additional benefits of alignment with the L1.

2.2 Hydrozoa

Hydrozoa is presented as a consensus protocol within the Cardano ecosystem developed to address scalability, particularly for decentralized applications (dApps) requiring high levels of throughput and fault tolerance Hydrozoa, 2023.

While no working implementation could be found, Hydrozoa claims to be specifically designed to improve the performance and reliability of consensus in environments with a large number of validators. It is aimed at enhancing Cardano's decentralized application layer by offering a framework for handling high-frequency, multi-node validation, which is a core requirement for real-time data oracles like Orcfax.

2.2.1 Hydrozoa against requirements

Challenges: While Hydroza presents itself as a compelling solution, and one which seems to address many of the key requirements addressed by Orcfax, the lack of any working code or implementations immediately rules out Hydroza as a solution.

2.3 Iagon

Iagon is a decentralized cloud computing and storage platform, built to leverage blockchain technology for distributed storage and compute resource management Iagon, 2023.

Iagon uses decentralized network infrastructure to store data in a secure, distributed manner. Its primary use case is in cloud-based applications where decentralized data storage and processing are prioritized over real-time consensus. This decentralized approach enables Iagon to deliver reliable storage services across a network without requiring a traditional high-speed consensus protocol, making it more suited to applications requiring data integrity and accessibility over rapid, consensus-driven data validation.

Iagon operates by distributing data across a network of decentralized nodes, and claims to be effective at protecting against data loss or tampering, by redundantly storing and managing data across the network Iagon, 2023.

However, a lack of available resources and information constrain the ability to say more about the solution; at the time of writing many links presented in the docs that would be helpful to explain iagon do not seem to exist. It is not entirely clear if it is, or will be, a sidechain or L2.

2.3.1 Iagon against requirements

Challenges: While Iagon presents itself as a compelling consensus solution utilizing a unique proof of storage architecture, the ability for Orcfax to assess Iagon's architecture and design against its own needs is highly constrained by the lack of documentation and working code. While the available docs are informative as to the solution's purpose, they are insufficiently technical or insightful.

2.4 Lodestar

Lodestar is a JavaScript-based consensus client for the Ethereum 2.0 Gasper consensus mechanism developed to implement Ethereum's Proof-of-Stake (PoS) consensus model through the Beacon chain Lodestar, 2023. As an Ethereum client, Lodestar enables nodes to participate in the Ethereum 2.0 PoS ecosystem, enhancing scalability and security while supporting Ethereum's transition from Proof-of-Work (PoW) to PoS. Lodestar primarily serves as a foundational client for Ethereum's staking and consensus layers, designed to handle transactions securely and efficiently in a decentralized network environment.

Lodestar operates within Ethereum's PoS framework, where validators secure the network by staking ETH and performing consensus duties. Lodestar's JavaScript architecture makes it accessible and versatile, although it is fundamentally tailored to Ethereum's ecosystem rather than cross-chain or for Cardano integrations. Lodestar, 2023.

2.4.1 Loadstar against requirements

Efficiency: Lodestar's PoS model on Ethereum is effective in supporting moderate transaction throughput, with some benchmarks showing between 1000 to 1250 TPS (Ethereum Hardware Resource Analysis Update, 2024), but its throughput capacity is limited by Ethereum's network constraints, which are different from Cardano's capabilities. The Beacon chain, while efficient within Ethereum, would require additional adaptation to meet the low-latency (T) and high-throughput (V) demands of Orcfax.

Reliability: Ethereum 2.0's PoS consensus model provides network security by requiring block finality to reach 2/3 consensus among nodes (What is Finality), which exceeds Orcfax's security and fault tolerance needs. However, its reliance on Ethereum's staking mechanisms and reward systems means that its security model is tightly linked to Ethereum's staking protocol, which may not fully translate to an Orcfax use case.

Challenges: The primary challenges with adapting Lodestar for Orcfax are its dependency on Ethereum's PoS structure and its limited throughput compared to Cardano's capabilities. While Lodestar's JavaScript-based design offers flexibility, its reliance on Ethereum's Beacon chain constrains its applicability for Orcfax, which requires faster and more flexible data consensus within the Cardano ecosystem. Integrating Lodestar might require developing custom bridge or cross-chain protocols and potentially redesigning aspects of its staking incentives.

2.5 Midgard

Midgard is presented as a protocol used within decentralized liquidity networks like Thorchain to manage and update liquidity states in real-time. The solution claims to be designed to facilitate high-throughput data handling in DeFi environments and for processing rapid liquidity changes across distributed pools, all while maintaining up-to-date state information for liquidity providers Midgard, 2023. Midgard also claims to implement byzantine fault tolerance (BFT), ensuring stability and consensus even in environments with malicious nodes.

However, a lack of available resources and information constrain the ability to ascertain how well the solution meets the needs of Orcfax; at the time of writing many links such as those for documentation and the whitepaper resolve to "what is Mitgard?", which provides insufficient information to say more.

2.5.1 Midgard against requirements

Challenges: While Mitgard presents itself as a compelling consensus solution, the ability for Orcfax to assess Mitgard's architecture and design against its own needs

is highly constrained by the lack of documentation and working code. While the available docs are informative as to the solution's purpose, they are insufficiently technical or insightful.

2.6 NEM

NEM (New Economy Movement) utilizes a unique consensus mechanism called Proof-of-Importance (PoI), designed to reward participants based on their activity and contribution within the network NEM Project, 2023. Unlike traditional PoW or PoS models, PoI evaluates network importance by factoring in a participant's transaction history, frequency of transactions, and network holdings, promoting active engagement and network utility. NEM's PoI model is primarily used within its ecosystem for facilitating transactions, but its unique activity-based approach to consensus offers an alternative to traditional staking mechanisms, prioritizing network participation over token holding.

In NEM's PoI model, participants earn rewards based on their calculated importance score, which is determined by an algorithmic assessment of transaction activity, account age, and other engagement metrics. This approach claims to discourages centralization by rewarding activity and connectivity within the network rather than relying on volume-based staking, as seen in some PoS models.

NEM's PoI nodes validate transactions and reach consensus without requiring significant computational resources, claiming that it's efficient for moderate throughput applications; however, specific figures to back this claim could not be found. The system's activity-based scoring method is intended to encourage nodes to remain active and to contribute consistently, thereby fostering a stable network with distributed validator incentives NEM Project, 2023.

2.6.1 NEM against requirements

Efficiency: NEM's PoI model is optimized for moderate transaction throughput, performing well for applications requiring steady transaction handling without the resource intensity of PoW or the latency which its docs associate with high-volume PoS networks. However, for Orcfax, which has identified high-throughput validation for real-time data as a requirement, NEM's capabilities may not fully align, as its focus on engagement-based incentives could limit its transaction speed and scalability in high-frequency scenarios NEM Project, 2023.

Reliability: By encouraging active participation over token staking, NEM's PoI model provides an alternative structure for data integrity. However, the reliability of NEM's PoI is highly contingent on user activity and engagement, making it less ideal for applications where consistent, rapid consensus is necessary regardless of participation patterns.

Challenges: The main challenge with NEM's PoI for Orcfax is its reliance on engagement-based incentives, which may not adequately support the high-throughput and continuous validation needs of a decentralized oracle network.

2.7 Raft-rs

Raft-rs is the rust implementation of the Raft consensus protocol, which is primarily used in distributed systems where consistency and reliability are prioritized over throughput and scalability Raft, 2023. Raft is designed for use in closed networks where trusted nodes operate cooperatively. The network elects a single leader among nodes, who then coordinates the validation and replication of data entries across follower nodes, ensuring consistency and data integrity. If the leader fails, a new one is elected to take over the validation and data coordination duties.

Raft's simplicity and leader-based model make it suitable for smaller networks where high levels of trust exist among nodes, but it may be less resilient in environments where malicious nodes must be accounted for.

2.7.1 Raft against requirements

Efficiency: Raft is highly efficient in terms of latency and resource use within small, closed networks where it can maintain high levels of consistency without the complexity of large-scale byzantine fault tolerance Raft, 2023.

Reliability: Raft is reliable for smaller networks where nodes trusted and cooperative, as its leader-election process ensures data consistency. However, in a decentralized oracle network with potentially adversarial participants, Raft's inability to accommodate malicious actors presents a vulnerability, especially where resilience against malicious nodes is essential.

Challenges: Raft's primary challenge as a drop in solution for Orcfax adapting lies in its closed, leader-based consensus model, which is incompatible with decentralized oracle requirements; the Orcfax network is being designed as a decentralized network and must be able to deal with malicious nodes

2.8 Avalanche

The Avalanche consensus protocol, utilizing the Snowball consensus algorithm, boasts a probabilistic, high-throughput consensus that emphasizes rapid, secure agreement despite adversarial conditions Avalanche, 2023.

Avalanche consensus, which includes Snowball, is designed to achieve consensus across a large number of validators by relying on repeated probabilistic sampling and gossip protocols. This structure makes it resilient, scalable, and well-suited to environments where high transaction rates and fast finality are critical, such as decentralized finance and data validation in oracle systems.

Snowball works through a process called metastable consensus, where nodes repeatedly sample one another to reach agreement on data validity. Nodes query others in the network to confirm decisions, using probabilistic algorithms to ensure convergence on a single outcome. This process allows Snowball to achieve consensus without requiring all nodes to agree simultaneously, reducing latency and enabling high throughput. The probabilistic nature of Snowball's consensus claims to allow the network to scale to thousands of validators without compromising security or speed Avalanche, 2023; this exceeds the requirements identified by Orcfax for throughput and scalability.

2.8.1 Snowball against requirements

Efficiency: Snowball's consensus mechanism is highly efficient, achieving fast transaction processing and finality with low latency. Its ability to handle thousands of TPS and its rapid consensus through probabilistic sampling exceeds Orcfax's high-throughput needs. Snowball's low-latency processing also aligns well with the requirements for rapid data updates in real-time oracle systems, as it allows data to be processed and validated almost instantaneously across a decentralized network Avalanche, 2023.

Reliability: Snowball's design includes resilience against adversarial environments, enabling it to handle up to one-third malicious nodes without compromising consensus integrity. This fault tolerance capability meets Orcfax requirements where maintaining secure data validation in an open network is a priority. The probabilistic sampling method Snowball uses reduces the impact of malicious actors by making it difficult for any small group of nodes to influence the network's consensus direction, ensuring reliable and secure data handling Avalanche, 2023.

Challenges: While Snowball exceeds many of the orcfax requirements, an Orcfax implementation could be labour intensive. Not only is the Snowball design in itself complicated, its operation within the Avalanche's network could mean additional complexities relating to bridging protocols.

2.9 CometBFT

CometBFT, formerly known as Tendermint Core, is the GO implementation of the BFT consensus protocol which is primarily used within the Cosmos ecosystem CometBFT, 2023. Known for achieving low-latency finality and high throughput, CometBFT is designed for blockchains requiring quick transaction finality, making it popular among interoperable and multi-chain ecosystems. It combines BFT consensus with PoS incentives to create a secure, decentralized structure capable of handling moderate-to-high transaction volumes in adversarial environments.

CometBFT operates through a two-phase BFT consensus model that allows validator nodes to reach agreement on the inclusion of transactions. Each validator proposes and votes on blocks, and transactions are finalized within seconds, ensuring quick data validation and low-latency processing. CometBFT is structured to handle both inter-chain and intra-chain communication, making it adaptable to multi-chain environments. Its implementation of BFT enables it to tolerate a significant portion of malicious nodes while maintaining consensus integrity CometBFT, 2023.

2.9.1 CometBFT against requirements

Efficiency: CometBFT is known for meeting low-latency (T) and high-throughput (V) demands of systems like Orcfax and can accommodate up to 180 nodes within a network(Validator Overview). With an optimized structure for block finality, CometBFT can handle moderate to high transaction rates while maintaining stability. This combination of efficiency and network size aligns well with Orcfax's core requirements.

Reliability: CometBFT's BFT consensus model provides robustness against adversarial conditions, enabling it to handle environments where up to one-third of nodes may act maliciously CometBFT, 2023. This level of fault tolerance is crucial for decentralized oracle services, where data integrity and resistance to malicious actors are paramount. CometBFT's resilience aligns with Orcfax's requirements for security and reliability.

Challenges: Integrating CometBFT with Orcfax may require adapting its block proposal and voting structure to align with the data validation and consensus needs of Orcfax. These adaptations are feasible within CometBFT's flexible design, but careful configuration would be necessary to optimize performance within Orcfax's real-time data processing framework.

2.9.2 Cardano-IBC

An implementation of CometBFT by Orcfax could provide future opportunities to leverage Cardano native tooling. The Cardano Foundation is developing Cardano-IBC as a framework for enabling Inter-Blockchain Communication (IBC) on the Cardano blockchain; Cardano-IBC focuses on creating secure, cross-chain interactions, specifically aiming for interoperability with ecosystems like Cosmos, which uses IBC protocols for secure cross-chain data and asset transfers Cardano Foundation, 2023.

IBC's claims regarding its capability of enabling efficient data exchange across networks with low latency, could be useful in the event of a CometBFT implementation by EchoNet. However, this solution requires further research to better understand how its implementation would affect an Orcfax implementation of CometBFT within EchoNet.

2.10 VeChainThor

VeChainThor uses Proof of Authority (PoA) for low-latency, high-throughput transaction finality, primarily in controlled environments VeChain, 2023 PoA enables fast transaction processing by relying on a limited number of trusted validators who are pre-approved, making it more efficient but less decentralized than PoS or PoW models. VeChainThor's PoA model is designed for enterprise applications, such as supply chain tracking, where rapid finality and controlled validator networks are prioritized over decentralization.

The VeChainThor network achieves consensus through selected validators who have authority within the network. These validators verify transactions and add blocks to the chain, enabling near-instant finality and high transaction throughput VeChain, 2023. However, PoA's reliance on a fixed set of validators introduces centralization risks, making it less suited for open, decentralized applications like Orcfax.

2.10.1 VeChainThor against requirements

Efficiency: VeChainThor's PoA model enables rapid transaction processing, allowing the network to handle high transaction volumes with minimal latency. This efficiency aligns with Orcfax's low-latency requirements but falls short in scalability within a highly decentralized environment, as PoA's performance depends on a restricted number of trusted validators. Therefore, while VeChainThor could meet Orcfax's throughput and latency requirements, its structure limits scalability and broader decentralization VeChain, 2023.

Reliability: PoA provides reliability through a fixed set of known validators, reducing the risk of malicious actors in a controlled environment. However, for a decentralized oracle, this model is less robust, as it lacks byzantine fault tolerance and is vulnerable if the trusted validators become compromised. For Orcfax, which requires resilience against adversarial behavior, VeChainThor's PoA may not provide the required reliability in an open network setting VeChain, 2023.

Challenges: VeChainThor faces numerous challenges for implementation by Orcfax. Adapting VeChainThor's PoA model to Orcfax's requirements could involve significant modification of validator selection and consensus structure.

3. Comparative assessment

The assessment of each consensus protocol has been organized in thee following table in order to aid in further comparison across Efficiency, Reliability, Scalability, and Challenges & Adaptions:

Protocol	Purpose	Strengths	Challenges
Hydra	L2 scaling for Cardano; enhances throughput and reduces latency through parallelized mini-ledgers ("Hydra heads").	Efficient transaction processing in parallel; connects to Cardano main chain for synchronized state transitions.	Relies on unanimous consent, vulnerable to a single malicious actor; participant count limit (57) does not meet Orcfax requirements
Hydrozoa	Designed for high throughput and fault tolerance in dApp environments on Cardano.	Aims to support high-frequency, multi-node validation, enhancing decentralized application performance.	No working implementation currently; claims not yet proven in live environments.
	Decentralized cloud computing and	Decentralized data storage and	Limited documentation and lack of

Protocol	Purpose	Strengths	Challenges
Iagon	storage, focusing on data integrity and accessibility.	processing, with protection against data loss and tampering.	implementation make it difficult to assess compatibility with Orcfax's needs.
Lodestar	JavaScript-based consensus client for Ethereum 2.0, supporting PoS and scalability.	supports 1000 to 1250 TPS and enhances security by requiring 2/3 consensus for finality.	Primarily serves Ethereum; may not align directly with Orcfax's specific requirements and complexity may inhibit implementation.
Midgard	Used in decentralized liquidity networks (e.g., Thorchain) for real-time liquidity management in DeFi.	Supports high-throughput data handling and byzantine fault tolerance for stability in DeFi contexts.	Insufficient documentation limits assessment; unclear applicability to Orcfax's real-time consensus needs.
NEM	Uses Proof-of-Importance (PoI), rewarding participants based on network activity and engagement.	Encourages active engagement and utility within the network, potentially fostering decentralization.	May not meet Orcfax's high-throughput needs; PoI model depends on user activity, possibly limiting speed and scalability.
Raft	Leader-based consensus model prioritizing consistency in closed, trusted networks.	Low latency and efficient resource use within small networks; ensures data consistency.	Not suitable for decentralized, adversarial environments; vulnerable to malicious nodes due to leader-based structure.
Avalanche	High-throughput probabilistic consensus using Snowball for scalability and resilience.	Scalable, resilient against adversarial conditions, suitable for high transaction rates.	Complex implementation may challenge direct application; requires adaptation for specific needs in Orcfax.
CometBFT	GO implementation of BFT consensus used within the Cosmos ecosystem for low-latency finality.	Quick transaction finality, supports inter-chain and intra-chain communication.	Primarily designed for Cosmos; adaptation needed for Orcfax-specific requirements.
VeChainThor	Enterprise-focused PoA consensus for supply chain and controlled environments.	High throughput and low latency, suitable for environments with trusted validators.	Limited decentralization; PoA may not align with Orcfax's decentralized requirements.

4. Conclusion

Based on the analysis of each consensus protocol and the initial Must Have requirements identified by Orcfax, none of the reviewed consensus protocols fully meets all of Orcfax's needs out-of-the-box. The most protocol that seems to best align with the requirements is Cosmos's CometBFT. In particular:

- Simplicity-(ish). Limiting the participants to 180 nodes allowed Cosmos/CometBFT to be simpler, than some of the alternatives. EchoNet is targeting only 100 nodes.
- Built as SDK. What for other solutions maybe considered "internal APIs", are external for CometBFT. This means the code and the ideas behind the code are much more accessible.
- Synergies. The development of the IBC by the Cardano Foundation provides a hope that there will be other tooling that we can take advantage of and contribute to.

4.1 Limitations

As stated at the outset, this paper did not attempt to cover the breadth of consensus protocols which have been deployed across the numerous blockchain networks active at the time of its writing. Instead, a limited sample of consensus protocols used by PoS blockchains were was selected.

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

4.2 Closing Thoughts

After assessing the limited sample set of consensus protocols against an initial understanding of Orcfax network requirements for EchoNet, several key takeaways became clear.

The most interesting lines of inquiry are with the CometBFT implementation of the Cosmos consensus protocol.

- CometBFT meets requirements on node count; it demonstrably handles at least 180 nodes which is more than enough as EchoNet will accommodate 100 Validators with licenses.
- Finality is faster than Ouroboros and exceeds our current understanding of EchoNet requirements.
- The tooling lacks the significant complexity that would impair an Orcfax implementation of another solution; this makes CometBFT a much more feasible starting point given time constraints.

An Orcfax implementation of a Cosmos consensus solution could make future Cardano-IBC tooling from the Cardano Foundation available and relevant to EchoNet design.

Additional research and analysis is needed to further appreciate the interplay between the implementation of a consensus protocol by Orcfax and its staking mechanism.