Figment Insider

Q1 2022 / **Issue 01**

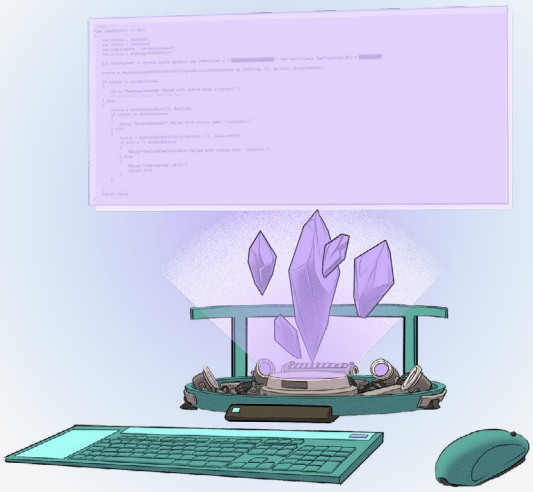
Foreword

As one of the leading staking providers, active on more than 60 networks, we are deeply involved with most major Proof of Stake protocols, and we dedicate our time to figuring out how things work.

This report highlights some of our work, as well as the unique perspective that comes from our research team's ability to compare and contrast a complicated and fascinating environment.

Proof of Stake has taken over the blockchain world, and will only continue to grow with the upcoming Ethereum merge. Read on to learn about the biggest trends, important upcoming changes, and what's coming next.

Table of Content



Ethereum Q1 2022 Report

- Nathan Workman, Senior Analyst

Summary:

- **Network revenue decreased 57.19% from Q4 2021** ($4.34B USD to $2.48B USD). As in Q4 2021, approximately 87% of these fees were burned and removed from circulating supply.
- **Average network transaction fees dropped 14.57% from Q4 2021** ($26.89 USD to $23.47 USD).
- Though transactional volume was down from Q4 2021, **average daily active addresses increased 3.98% in Q1 2022 (572,700 addresses to 595,473 addresses).**
- Aided by the reduction in gas fees on the network, **circulating supply increased 1.0256% over Q1 2022** (118,958,024 ETH to 120,178,122 ETH).
- Despite significant market volatility, **total amount staked increased 19.1828% in Q1 2022** (8,818,933 ETH to 10,510,653 ETH), equating to 8.7459% of circulating supply.

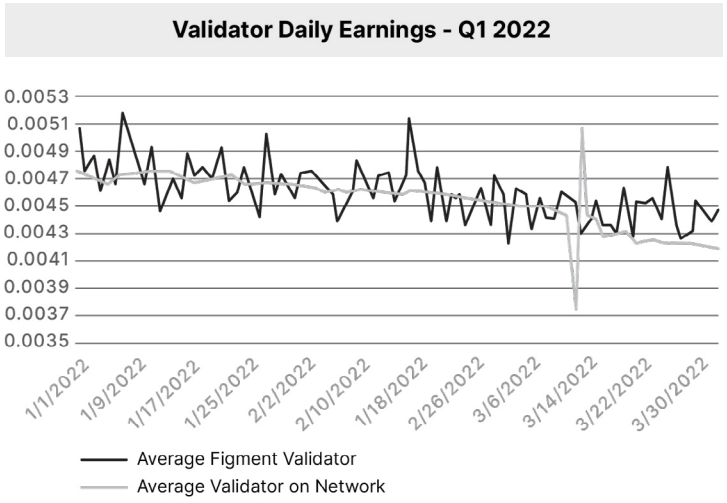
Insights

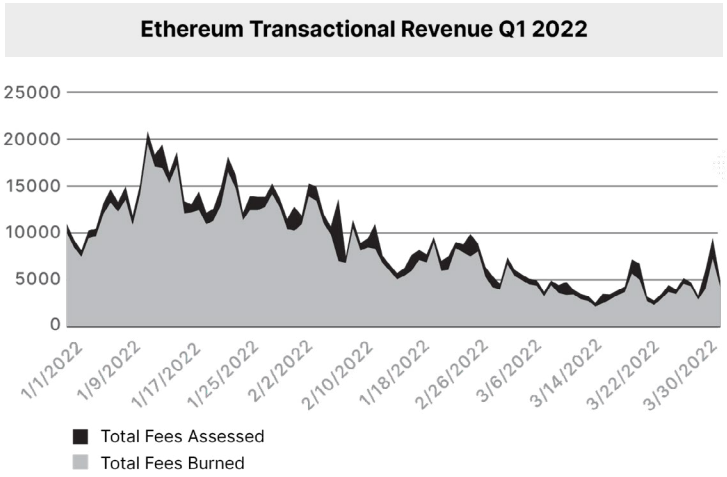
Average validator daily earnings decreased over Q1 2022, largely due to both a decline in transactional volume and an increase in the number of validators, which grew from 275,880 to 328,461 over the period.

This is significant, since under current protocol parameters, once 327,680 validators are added to the active set, the number of validators that can be activated each epoch increases from 4 to 5 (or 900 per day to 1,125 per day), and one additional validator slot per epoch will be added for every 65,536 validators that are added to the active set.

Transactional fees were slightly lower over the entirety of Q1 2022 compared to the previous quarter. However, the average fee dropped considerably during the quarter. The average fee was $36.19 in January, which declined to $21.89 in February, and which further declined to $11.74 in March. Despite this drop in transactional volume and fees, no changes were made to modify the parameters of EIP-1559, thus approximately 87% of these fees were burned.

> Though network revenue decreased over the quarter, Figment's validators consistently earned more than an average validator on the network.





Over the entire quarter, Figment's Validators earned 1.2991% higher than an average validator on the network, and the gap increased as more validators were added to the active set:

Month	Average Validator Earnings	Average Figment Validator Earnings	Difference
January	0.145688 ETH	0.146943 ETH	0.8617% Higher
February	0.128629 ETH	0.129465 ETH	0.6500% Higher
March	0.134933 ETH	0.138158 ETH	2.3901% Higer

All data sourced from: https://beaconcha.in and https://beaconscan.com.

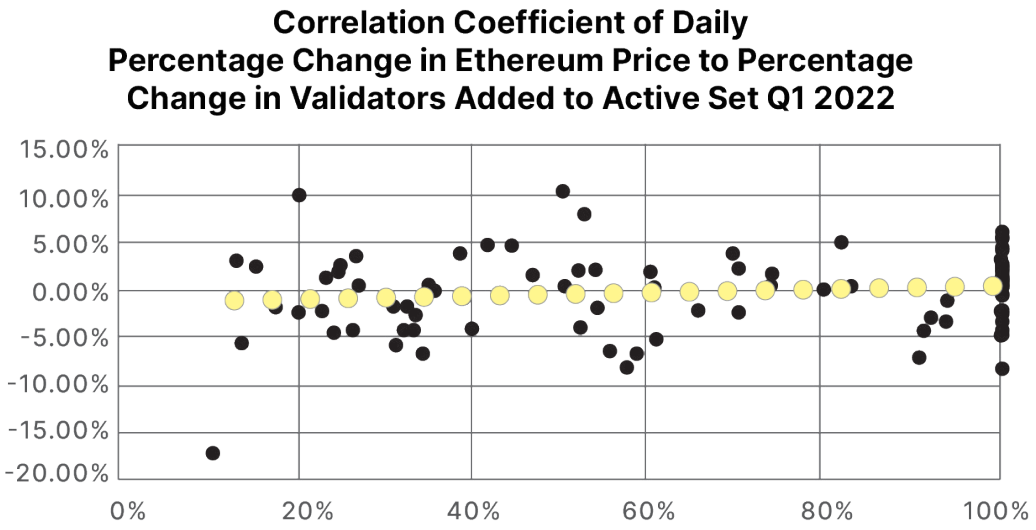
Token holders staked at a faster rate over the quarter, and price action on exchanges had little to no impact on staking rates.

Towards the end of the quarter, the number of validators added to the active set per day dramatically increased. In January, the maximum number of validators that could be added to the network was reached once (1/25). In February, this happened twice (2/24 and 2/25). However, in March, this happened in all but two days. This sustained increase in the rate of validators being added to the active set has created an activation backlog, which is approximately two weeks at the time of this report. The month-to-month data is as follows:

Month	Average Validators Added Per Day	Percentage of Maximum Validators That Could Be Activated
January	447.74 Validators	49.7491%
February	413.32 Validators	45.9246%
March	895.45 Validators	98.7397%

All data sourced from: https://beaconcha.in and https://beaconscan.com.

This increase in the rate of validators being added to the active set is almost certainly due to anticipation of increased staking yield after the Merge, not price action. The correlation between the day-to-day change in market price of Ether and the change in validators added to the active set over the quarter has an r-value of 0.13212, which is not statistically significant.

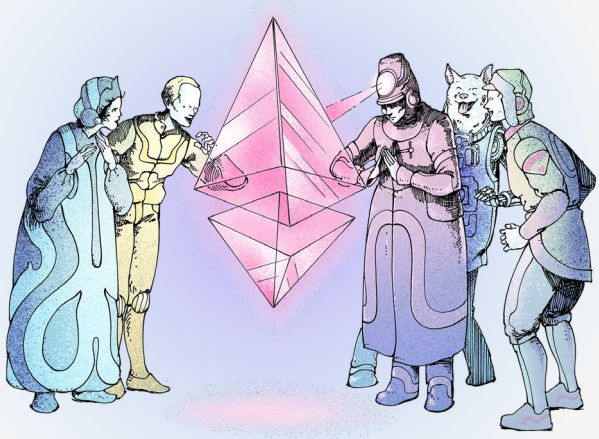


All data sourced from: https://beaconcha.in and https://beaconscan.com.

Since all validators must have an effective balance of at least 32 ETH to be added to the active set, the increase in validators is primarily responsible for the amount of Ether staked to the network having increased by 19.1828% over Q1 2022. This corresponds to a significant increase of the total supply of Ether staked, from 7.4643% to 8.7459% of the circulating supply.

If the staking demand holds at current levels leading up to the Merge, total supply of Ether staked would increase to approximately 11.6319% of the circulating supply by the end of Q2 2022.

All data sourced from: https://beaconcha.in and https://beaconscan.com.



The Risk of Client Concentration on Ethereum

- Benjamin Thalman, Research Analyst

The very fact that client diversity has become a hot topic in the **Ethereum** community is a sign of Ethereum's maturity and robustness. There are few (if any) other networks that have multiple clients. With that said, client diversity is an issue which has the potential to affect all Ethereum stakeholders. When client software goes wrong, outcomes range from mild - possible missed rewards for validators due to downtime - to catastrophic - the forking of Ethereum or the acceptance of a fraudulent state as canonical.

The impact of a bug or vulnerability in the code of a particular client depends on the percentage of users running that client:

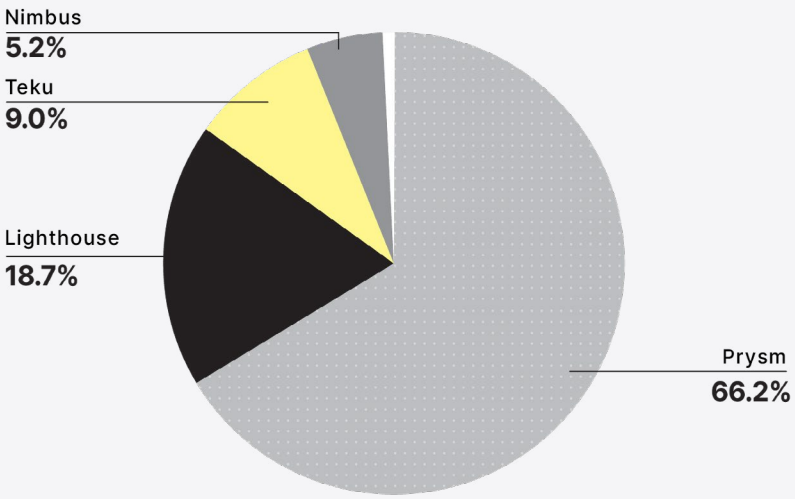
- Less than 1/3 of validators running specific consensus client: minimal impact - validators running this client will suffer downtime penalties
- Between 1/3 and 2/3 of validators: inability to finalize, inactivity leak (higher downtime penalties) until affected validator balances collectively drop below 1/3
- Around 50% of validators: potential fork
- Greater than 2/3 of validators - worst case - erroneous "fork" becomes canonical chain

(For more on client diversity see here)

Here is what consensus layer diversity has looked like recently:

This chart represents the percentage of nodes running various client implementations (i.e., 'clients') of the Beacon chain. Clients verify all transactions in each block, keeping the network secure and accurate.

Happily Prysm is just under the 2/3 threshold outlined above; in fact, the number looks to be even lower recently. For the time being this rules out a catastrophe. But Ethereum is a far cry from the ideal scenario of equal distribution across clients.

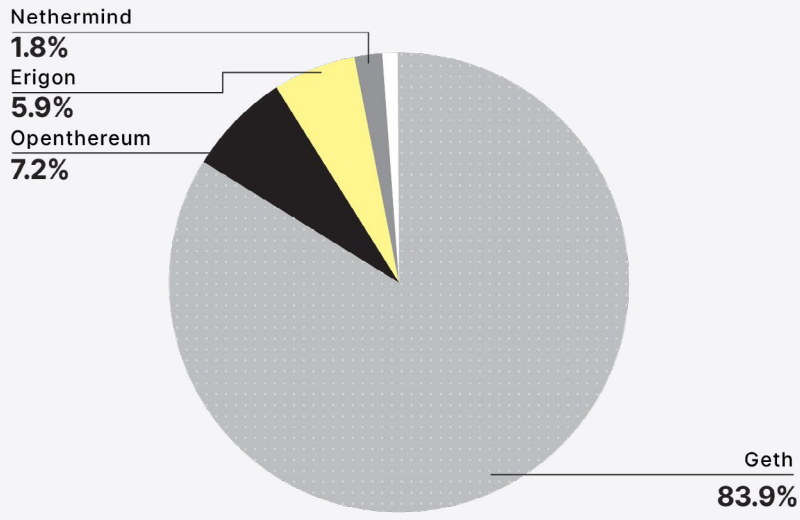


Source: https://clientdiversity.org/

> Although most client diversity conversations center on the consensus layer, diversity of the execution layer is also important:

This chart represents the percentage of nodes running each client implementation on Ethereum mainnet (also referred to as Eth1 or the execution layer).

Clearly this is not as diversified as the consensus layer. It is unlikely that this will change significantly until post merge, at which time it will be necessary to reassess the situation and encourage diversity as needed.



Source: https://ethernodes.org/

What can be done

Technical solutions

Obol is building distributed validator technology for Ethereum that divides the work of running a validator among multiple participants, so that if one participant goes down the rest of the group continues to perform; the group is called a Distributed Validator Cluster.

It is important to note that nothing precludes a user from participating in multiple Distributed Validator Clusters. This way, someone running a minority client can be encouraged to participate more, changing the effective proportions of client usage on the network.

Stakeholder Engagement

Stakeholders are increasingly realizing the importance of client diversity and are working to solve the problem:

Source: Twitter thread

Source: Twitter thread

Large entities should be encouraged to make their opinions on Ethereum client diversity known and public discussions between all stakeholders should be encouraged. Rated.network has a useful dashboard of large entities and the clients they are using:

Entities | Operators | 1d | 7d | 30d | All

Entity	Network Penetration	Client Distribution	Participation Rate	Eff. Rating
Lido	27.02 %	40.9 / 42.8	99.53 %	96.9 %
Coinbase	16.03 %	75.9	99.05 %	95.73 %
Kraken	9.4 %	90.3	99.47 %	96.59 %
Binance	5.53 %	68.9 / 26.2	99.77 %	96.38 %
Bitcoin Suisse	2.3 %	99.8	99.84 %	96.27 %
Staked.us	1.51 %	49.1 / 48	99.43 %	95.68 %
Rocketpool	1.46 %	42.3 / 33.2 / 16.6	98.55 %	95.38 %
f2pool.eth	1.01 %	99.8	99.81 %	96.9 %
Bitfinex	0.92 %	91.7	99.86 %	97.02 %
Huobi	0.82 %	93	99.94 %	97.19 %
wedex.eth	0.69 %	99.6	99.85 %	97.31 %
Bloxstaking	0.69 %	67.9 / 27.7	98.84 %	94.77 %
Ankr	0.64 %	95.1	96.89 %	87.88 %
Stakewise	0.49 %	65.6 / 30.5	99.86 %	95.79 %
Stakefish	0.44 %	96	99.84 %	97.09 %

Next page >

Source: Rated.Network

Client diversity is an important issue and deserves the attention of all stakeholders. It is a challenge that will be best solved by fighting on multiple fronts.

Client diversity is the responsibility of all stakeholders - not just the larger ones. But in the short to medium term, convincing larger entities to diversify their clients will have the greatest impact.

The Journey to 1000 blockchains begins with IBC

- Christopher Raddings, Protocol Analyst

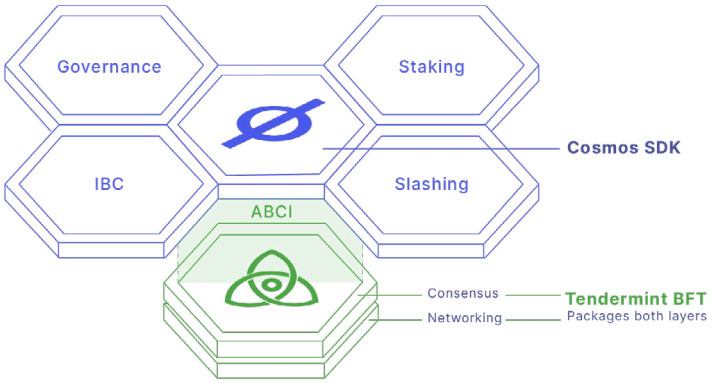
Cosmos is a multi-billion dollar ecosystem carrying out an ambitious, multi-layered, multi-chain, and cross-chain vision. How is this ecosystem growing? At what pace? And what converging events are we likely to see in the future that spur even greater ecosystem growth?

What comprises Cosmos's technology stack?

Tendermint Core
Tendermint Core is a byzantine fault-tolerant consensus mechanism with rapid throughput and immediate transaction finality upon block inclusion.

Cosmos SDK
The Cosmos SDK is a software development kit for blockchains and projects in the Cosmos ecosystem known for its modularity.

Inter Blockchain Communication (IBC)
IBC is a protocol standard that enables cross-chain communication and interoperability in a trust-minimized fashion between disparate blockchain zones.



Cosmos Growth

The Cosmos ecosystem continues to grow at an anabolic rate- with more prestigious projects coming out of the ecosystem, more IBC-enabled zones launching, more TVL locked, more IBC transfers, and more new accounts made than ever before.

ATOM Accounts and Delegation Growth

	January 1st	March 1st	Overall Increase
ATOM Accounts	659,204	990,512	331,308
ATOM Delegators	191,170	350,702	159,532
ATOM Transfers (previous 30 day period)	2,867,496	4,464,798	1,597,302

Figure 1 / Source: https://cosmoscan.net/cosmos/network-stats

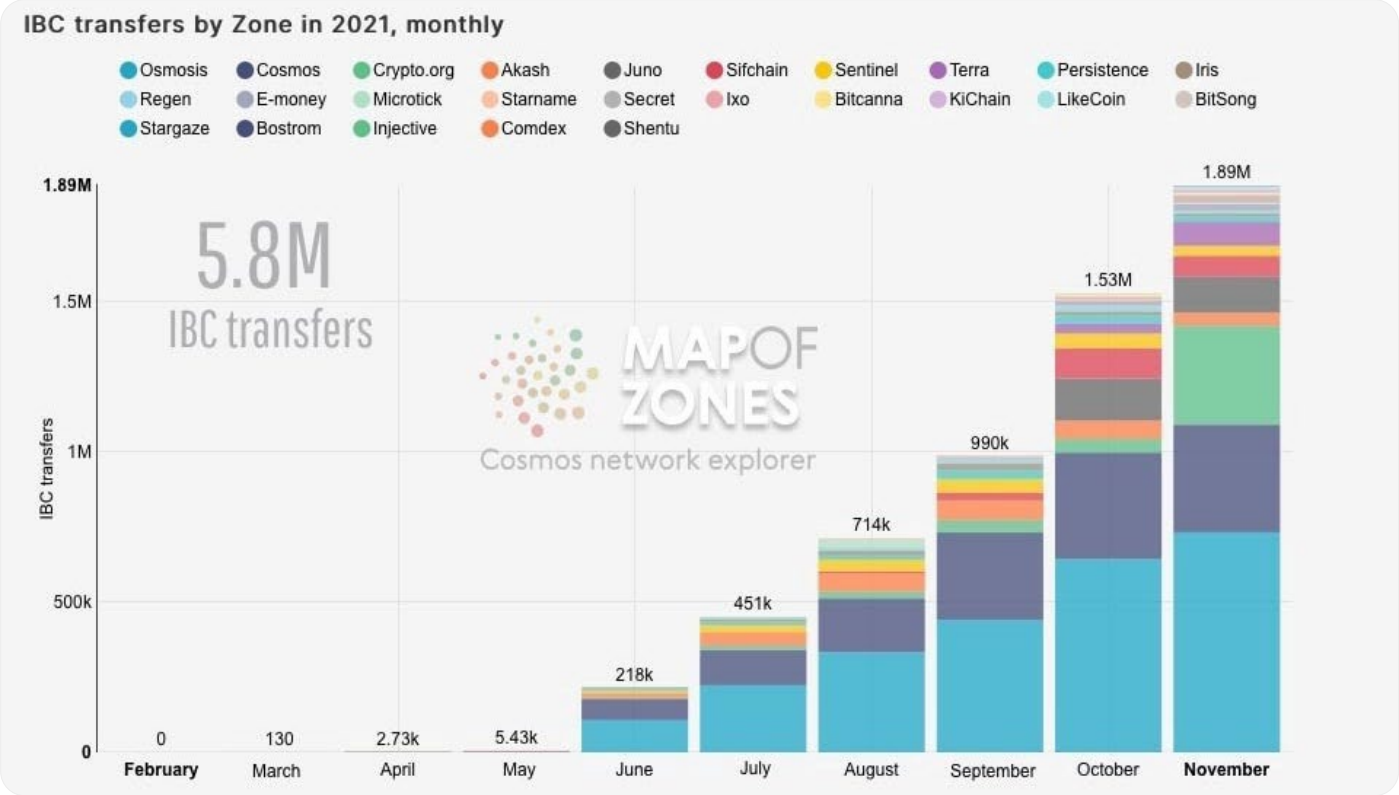


Figure 2 / Source: Medium Article

Cosmos Ecosystem Growth Metrics (March 1st- March 31st)

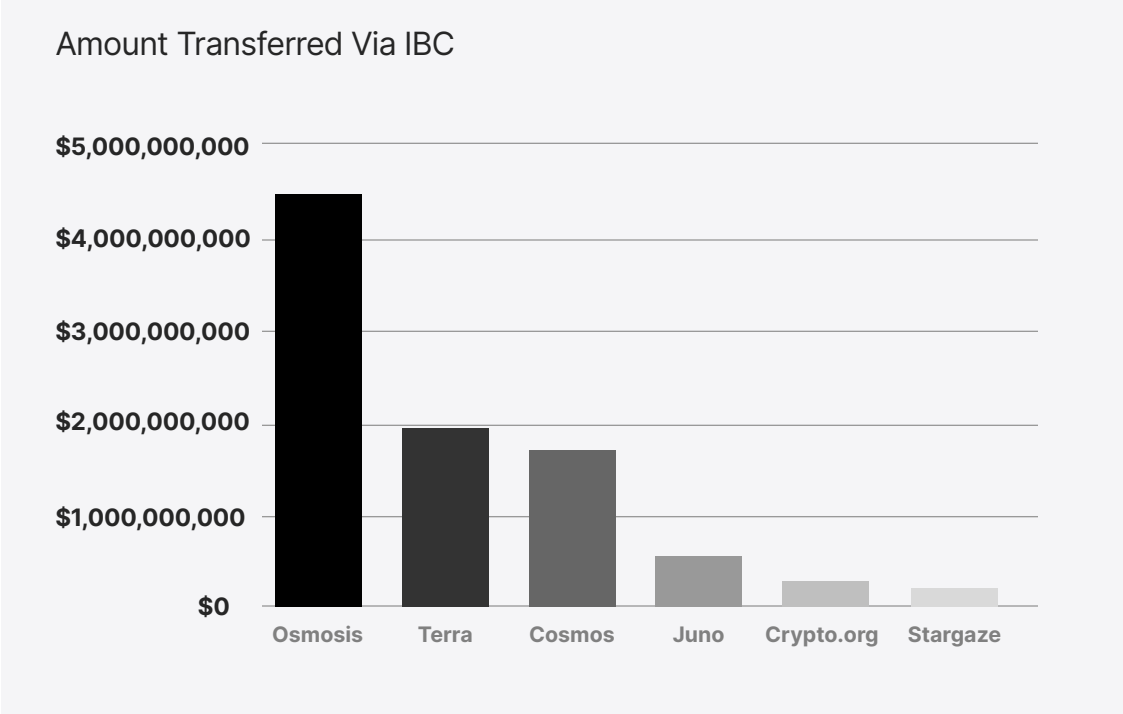


Figure 3: Amount Transferred Via IBC (March 1st- March 31st)
Source: https://mapofzones.com/?testnet=false&period=720&tableOrderBy=ibcVolume&tableOrderSort=desc

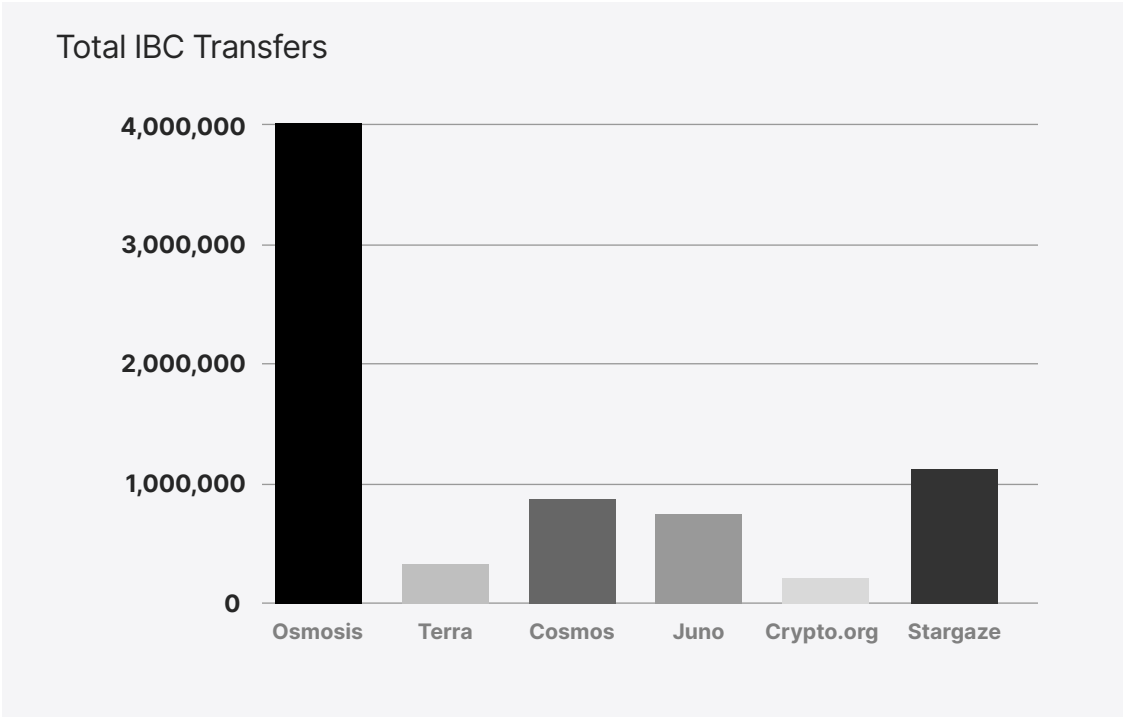


Figure 4: Total IBC transfers (March 1st- March 31st)
Source: https://mapofzones.com/?testnet=false&period=720&tableOrderBy=ibcVolume&tableOrderSort=desc

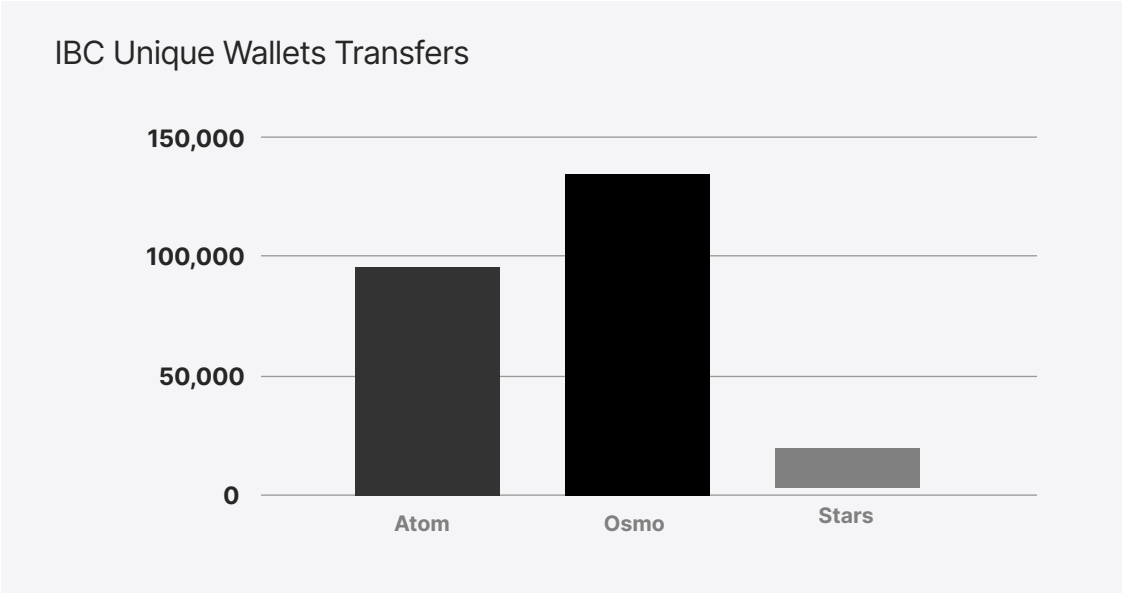


Figure 5: IBC Unique Wallets Transfers for ATOM, OSMO AND STARS (March 1st- March 31st)
Source: https://mapofzones.com/?testnet=false&period=720&tableOrderBy=ibcVolume&tableOrderSort=desc

Cosmos Ecosystem Growth and IBC Growth

IBC functionality will see further upward propulsion with the advent and adoption of features such as interchain accounts. Interchain accounts are an extension of IBC functionality because they expand the uses of IBC beyond just token transfers and allow for novel ways of cross-chain coordination and interaction, such as controlling accounts on separate IBC blockchains, running truly cross-chain DAOs and the creation of new inter-chain wallet products. It will also make account creation more user-friendly. Even without upgrades, overall IBC transactions and IBC value transfers in total dollar amount will rise as such standards and features become a commonality in the Web 3 space and IBC gains a further foothold.

Predictions For The Future: An Acceleration Of The Exponential Trends

Centralized bridging solutions will lose their dominance in the long-run due to them being an economically concentrated attack vector, and trust-minimized cross-chain standards such as IBC will become ubiquitous. Other key players in the interoperability and cross-chain space, such as Polkadot and Avalanche, will likely plug into IBC, weaving intermeshing layers of interoperability between IBC-enabled Cosmos SDK chains, Parachains, and Subnets. Kusama-esque perma-testnets will allow blockchains, dApps, DAOs, and DeFi experimentation to flourish by the thousands. Many horizontal scaling solutions will be implemented to accommodate more frequent usage and mainstream adoption.

Furthermore, many new projects are likely to garner significant network effects, such as Agoric, Umee, and Sommelier. They will further bolster the TVL locked into the Cosmos ecosystem, in the same way that newcomer network Stargaze has become the 7th most popular chain for IBC transactions.

Similarly, the TVL in the Cosmos ecosystem will continue to expand as new innovative and organic blockchains unfurl at a lightning rate. Game-changing Layer 1s such as Archway and Celestia will come to Cosmos and bring even more value into the ecosystem.

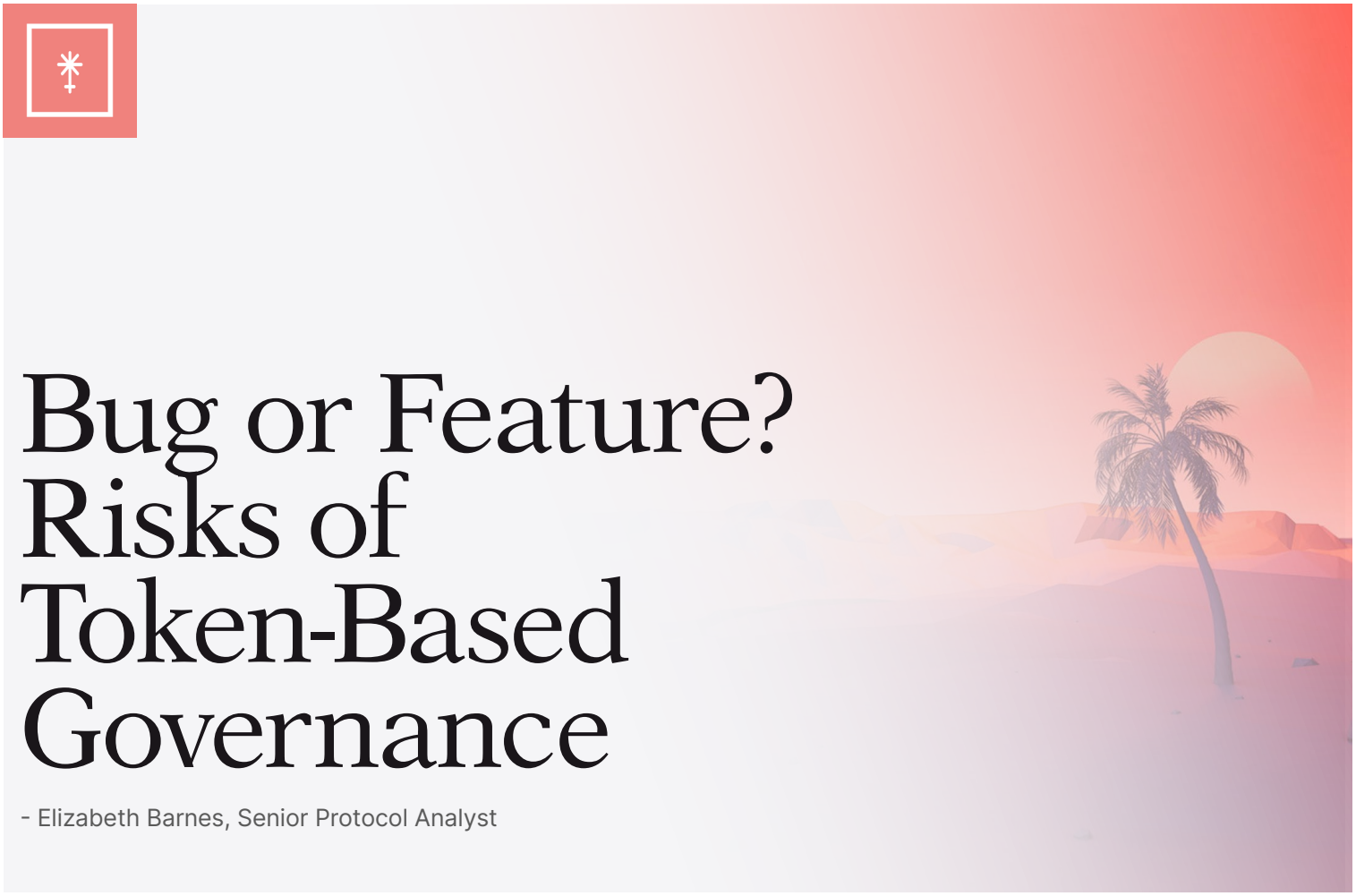
IBC Connected Zones

The Cosmos ecosystem is growing exponentially, with a multitude of blockchains interconnecting via IBC every month. From January 1st, 2022, to March 31st, 2022, the number of active zones (IBC connected blockchains) increased by 15 and went from 28 to 43, with many other zones anticipated to rocket forward in the next quarter.

Looking Ahead For Cosmos

Cosmos will continue to expand and flourish with more Layer 1s, dApps, and IBC transactions than ever before. Cosmos will keep growing in terms of interoperability and connectivity irrespective of the macroeconomic conditions. IBC-enabled zones will continue to proliferate, and we expect these zones to continue along the aforementioned exponential trajectory, thus proving that the journey to a 1000 blockchains begins with a single IBC connection.

Bug or Feature? Risks of Token-Based Governance



- Elizabeth Barnes, Senior Protocol Analyst

The Juno network launched a governance proposal this quarter, alleging that a large token holder had gamed the stakedrop of Juno tokens and received more than what they were allocated.

The proposal suggested that the chain clawback those funds, leaving the whale with the maximum amount of JUNO in their account they qualified for. In order to do so, the network would have to stop the chain, roll back the chain to a particular block height where the whale did not have those funds, and then restart the chain.

> Proposal 16 is a threat to one of the core tenants of blockchains: immutability.

Total: 11,126,664.888142 JUNO

YES
7.12%
792,405.063828 JUNO

NO
56.36%
6,270,962.643919 JUNO

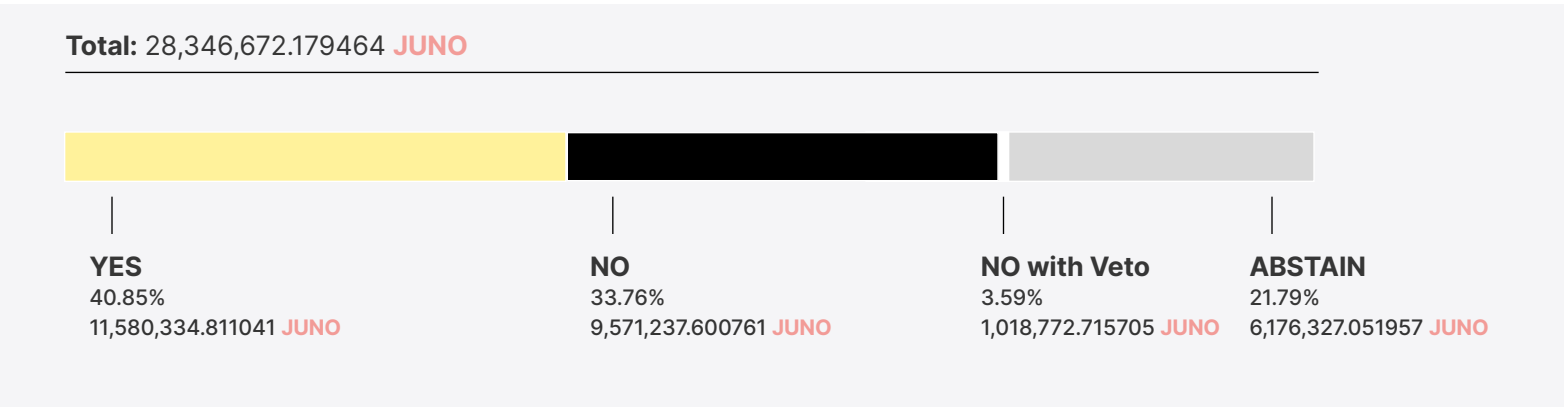
NO with Veto
0.68%
75,129.189245 JUNO

ABSTAIN
35.84%
3,988,167.991150 JUNO

In August 2021, Juno announced a stakedrop, and as a part of the rules, they instituted a "whale cap," where those staking more than 50k ATOM would not receive more than the maximum amount of JUNO, $50k.

A few months later, a JUNO token holder introduced proposal 4, suggesting that there was an account that "gamed" the stakedrop. They reported that this account received 2.5 million JUNO - above the maximum $50k allocated. This proposal suggests that the community blacklists/deletes 90% of JUNO in the account. The community overwhelmingly voted No on this proposal.

Then, on March 10, 2022, a JUNO stakeholder launched proposal 16. It repeated the allegation as stated in Prop4: that one account gamed the stakedrop and proposes reducing those funds to $50k. The whale in question has denied these allegations. We voted NoWithVeto. 97% of all staked tokens voted on this proposal, a very rare experience.



The second proposal, proposal 16, and the potential implementation undermine the perceived trustworthiness of a chain. The chain will have to roll back the state to a time before the account had those funds and restart the chain. Prop16 was a signaling proposal, so there will need to be another governance proposal that acts on its intent. The implementation will require either a hard fork or an upgrade that is not backward compatible and launch the chain with the state altered to reflect the whale's new balance.

Usually, when hard forks happen, node operators who create blocks choose to either remain on the old version with the other state or upgrade with the new chain. A few years ago, when Ethereum hard forked, we got two separate chains: Ethereum and Ethereum Classic. This forces users to "vote with their feet " and choose one chain to migrate their activities.

Blockchains, in theory, are immutable. Chains are supposed to be large databases that record and track transactions. This immutability protects that information from corruption or alterations. This proposal violates that principle.

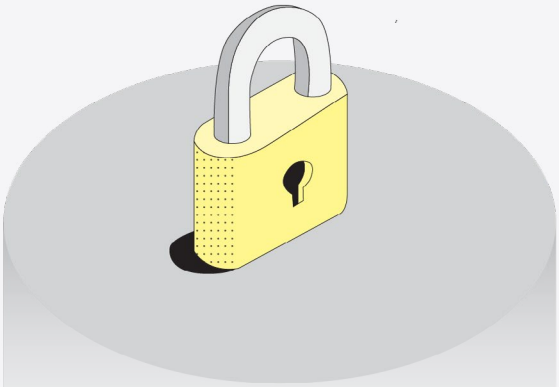
Blockchains are supposed to be trustless or trust minimized. If immutability means there should be a strong guarantee that account balances are not changeable by other parties so entities can transact confidently, then Juno is no longer trust minimized, and other chains with this type of governance are vulnerable to communities being able to alter the state of a chain.

If chains are no longer immutable, this changes the core value proposition of blockchains. To preserve the immutability of a chain, they must have a form of governance, or a community code of conduct that can uphold the ability of the chains to maintain a trust minimized environment.

Figment Performance

- ETH
- Yield changes overtime
- Uptime, attestation effectiveness, and comparison vs market

What does immutability mean in a world where chains can be rolled back at the behest of an outraged community?



The Year of Zero-Knowledge

- Clayton Menzel, Head of Protocols & Opportunities

Recent developments around zero-knowledge proof (zk proof) technology could be the answer for both. A **zk proof** is a basket term for a group of protocols that allow for one party (prover) to prove to another party (verifier) that their transaction, identity, or credentials are valid without the prover needing to reveal the information in order for the verifier to verify it.

Two of the most common questions asked in Web 3 are:

> How can we create scalable decentralized execution environments that can outperform their decentralized counterparts?

> Why the f*ck are all of my transactions publicly visible to anyone with an Internet connection?

The use cases for privacy seem pretty obvious... I, as a user of a zk proof protocol, would be able to freely transact and access data without having to disclose additional information about my transaction or identity, but how does this technology solve for scalability?

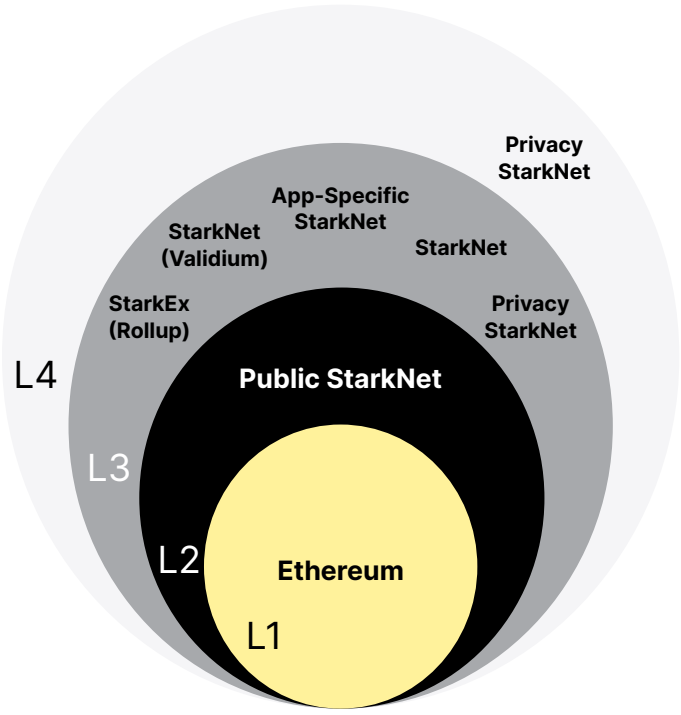
zk Proof Layer 2s

The scalability potential of zk proofs lies within the proofs themselves. These proofs are exponentially smaller than the data they represent, which in turn, makes them significantly cheaper to verify.

Starknet, a zk proof Layer 2 on Ethereum, is planning to build additional rollups on their layer 2, which could theoretically achieve near-infinite scalability while offering the security guarantees of Ethereum.

The vertical scalability zk proofs can offer a unique scaling solution not seen in horizontal scalability (i.e. additional Layer 1s like Solana & Avalanche connected via bridges), but it doesn't come without tradeoffs... finality on zk proof rollups can be much longer than on protocols leveraging a Tendermint consensus (minutes vs. seconds).

That said, this zk proof technology is in its nascent yet very much in its production-ready stage of its existence (even EVM compatible on zkSync), and offers a huge value proposition in its ability to preserve digital privacy.



A Layered Ecosystem

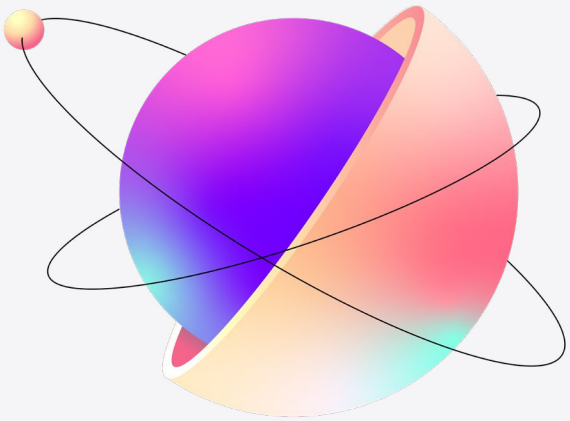
Fast, Scalable Privacy

Creating a universally accessible, antifragile, and non-corruptible Internet without privacy is impossible, and privacy is one of the few missing links in Web3 functioning at scale. Recent events like the Canadian government freezing bank accounts of individuals linked to political protests have shown the need and ultimate value of decentralized private money and communication networks.

Idealism aside, privacy is absolutely necessary for further institutional adoption. Privacy allows institutions to create truly open banking applications and financial services without having to expose individuals personal information. This allows for truly global and universally accessible markets that offer individual protection at the protocol level.

By leveraging zk proofs, protocols like Aztec, Anoma, Mina, and Penumbra can create fast, scalable, and privacy-preserving protocols designed to be a counterbalance to the ever intrusive nature of governments and tech monopolies in our daily lives.

Edward Wilson said humanity has, “Paleolithic emotions, medieval institutions, and godlike technology”, and if we want to continue building godlike technology, it should be used to protect the sovereignty of individuals from entities trying to become deities.



Celestia: A Gateway to the Modular Blockchain Stack

- Park Feierbach, Protocol Onboarding Lead

Q1 of 2022 brought into sharper focus a hefty shift in the design of core elements within the blockchain stack: a shift from monolithic blockchains that included execution, data availability guarantees, and consensus all in the same technological stack, to a modular paradigm in which these elements are abstracted into separate, purpose-built modules.

A modular thesis for blockchain architecture argues that taking apart pieces of a blockchain results in more efficient data management, since they normally process intensive efforts made on a single chain can be committed to multiple, radically altering the design space available.

At the center of much of this conversation has been **Celestia** (formerly LazyLedger), a data availability blockchain that removes and resolves the need for storing execution data on the same chain upon which you're performing the execution by providing probabilistic guarantees on the execution having happened.

In the modular paradigm, another chain (or rollup) can use Celestia to prove that the execution information for its transactions are 'available' using Celestia, freeing up space on the execution chain to do what it does best, and quickly, independent of the need to maintain its own execution data - but this would only be one potential implementation of a modular stack.

The appeal of a modular chain architecture becomes pretty intuitive when we compare, say Android and Apple mobile environments: Apple is a fiercely monolithic entity, keeping all of its information within the same stack often to great positive effect. Because of this, however, a tech stack like Apple's lacks flexibility, since all the pieces are integrated.

Android, by contrast, has always focused on a modular approach to expanding their market share. While Google itself is not an open source organization (Android OS is open-source), AndroidOS has the larger market share worldwide because it can be built to suit the needs of whatever implementation requires it, whereas Apple can't. More importantly, it allows builders to iterate on what they want to produce continuously to find what works.

With this said, Apple has also been able to focus on guaranteeing that all elements of their tech stack work together with extreme efficiency, which is part of what built out the brand's value and has preserved their place in the market - the issue here is that major breakthroughs can be a slow, tedious process.

Abstracting blockchain layers,% Alex Beckett on Celestia.org

From the perspective of modular blockchain architecture, this is where the analogy with Apple and Google may end. In theory, abstracting the many other parts of a particular stack (consensus, execution, tee-mining, data availability, etc) means providing agnostic services to one another, rather than a single chain doing all of these elements on the same chain.

A potential pitfall here would be interdependencies - where one or several execution chains depend on a modular element of their stack, a vulnerability of failure in this single modular element could lead to issues on the implementations that require it.

All the same, since a closed ecosystem doing all of these elements on the same chain means that your environment might become limited in both capacity and utility, the argument for a modular architecture is actually quite strong - though if a closed stack works better than a modular one, the monolithic paradigm might be preserved.

Understanding Data Availability and Sampling

Let's say that in theory, you own a factory that produces a widget, and that part of your product offering is that you do all of your widget production in the factory, without outsourcing any elements. This is the promise that you make to your customers - because it's a statement about the quality of the widget you are selling. You want your customers to be able to trust that you are indeed building your widget in the factory by providing strong guarantees that the widget is being made in the factory.

There are a number of ways that you could do this - the most obvious being that each time you make a widget for a customer, you invite them along for the ride, to watch the widget being made along the production line so that they can trust that you are the one making it. Obviously, this is quite process intensive for both you and the customer - both of you have to go through the work of surveilling the process in order to trust your guarantee that you make the widget in-house.

The simpler alternative would be installing a series of cameras along the production route that your customer can access whenever they want, so that any willing party can 'sample' a portion of the production process. This minimizes the effort necessary for you as the factory owner and the customer as a trusting party in 'believing' that your factory can keep its promise of producing everything in house, being that the widget is indeed made in-house and your willingness to make this apparent makes this truth 'available'.

Under a data availability paradigm, transactions that are executed on an execution layer dump the evidence of execution onto a Data Availability layer, and then use a probabilistic method known as 'sampling' using smaller chunks of data at a sufficient size to prove that the execution data exists, thereby allowing you (and anyone) to 'trust' the result was executed. The sampling is done by a number of 'light clients' that are the security cameras in our factory analogy. The question is: How many security cameras would be enough for you to trust that the factor owner isn't hiding part of the process?

It turns out that with a data availability layer, you only need to sample the block for inclusion about seven times until you have 99% certainty that the executed transaction was run, and that data of that execution was included in what was posted to the data availability layer. Any samples beyond this first 7 is proving the last 1% probability that the data was included in the block - which is a diminishing return on the effort.

This is the rule that gave Celestia its 'original' name - a ledger with 'lazy' guarantees to prove the availability of the underlying transactions, greatly improving the efficiency of proof.

This is not limited to data availability, either - a modular approach also opens up space for parties to build app-specific chains that can be used in any variety of methods, exploding the design space for other ways to build blockchain implementations between the service offerings of any one chain, and to iterate quickly with a high margin for scalability and failure tolerance.

This is the core value proposition of modularity: flexibility in constructing your implementations in exactly the ways that fit your needs, while outsourcing the elements you don´t want to worry about to other parties that do it better than you do.

Be your own bank, they said...

- Gavin Birch, Protocol Opportunity Specialist

Cryptocurrency advocates say **“be your own bank”** like it’s a good thing, but right now that’s not exactly easy or safe to do. It’s especially not easy because you may often have to choose between keeping your private keys handy or keeping them inaccessibly safe.

Rather than assume the risks involved in self-banking, investment firms and other institutional token owners often opt to use third-party custodian services to secure their assets. This makes sense, because they own non-trivial percentages of the entire token supply that must be protected from unwanted transfer or loss.

But token owners also need to easily stake, vote, and manage their tokens in various other ways. And the phrase "not your keys, not your crypto" comes to mind, because you often can't do the things you're invested in doing when an intermediary is controlling your private keys.

Perhaps there's another way

How can one safely transact with their primary account to manage daily token staking, voting, borrowing, and lending functions without exposing the private key? There are two potential solutions in the works. There's Qredo, whose team is aiming to launch a wallet and decentralize their network. And there's Entropy, whose team will be aiming to have their protocol integrated into the most popular wallets.

Two very different approaches. Qredo will begin with a hosted wallet with many carefully managed controls (to appeal to the accountability needs of large token holders), before gradually decentralizing their product. Entropy will make no concessions on decentralization, targeting existing wallets that support small to mid-sized token holders. Both Entropy and Qredo will offer cross-chain interoperability, which should become ever more important to manage their assets as the Web3 universe expands across many different chains.

In addition to the potential for cross-chain features, access control features will enable people to use the entirety of their assets to manage everyday functions (like managing token staking, voting, borrowing, and lending), without exposing their private keys. Decentralized custody solutions will also likely enable whitelisting accounts, setting spend limits, and any other number of access controls that prevent catastrophic outcomes, while still ensuring a smooth user experience. Here, mobile phones might be a strong option when thinking about a decentralized custody future.

Perhaps one of the most intriguing possibilities is that decentralized custody could enable automation that just isn't possible now, at least not with your entire treasury. Automating cross-chain transactions could be the next step for innovation, potentially a composable new development layer for new decentralized treasury management tools and more.

Regardless of what your bet is, a standard of decentralized custody will emerge as the next gold standard for key management. The sooner that we have reliable, secure, decentralized custody, the sooner we can pave the path to a better Web3 user experience.

The challenge is to make using your tokens easy, while making it hard to have your assets lost or stolen.

Conclusion

Q1 2022 has proven to be an excellent quarter for the Proof of Stake ecosystem. With over $260B in assets staked at the end of March, staked assets now represent ~12.5% of the global cryptocurrency market cap.

Thank you to all of our researchers who helped create this document, our developers who keep things operating, and everyone at Figment who values what Proof of Stake can accomplish.

To stay ahead of the DeFi curve and dig more into the staking ecosystem,

Contact our sales team to learn more about staking

Subscribe to our monthly newsletter

Follow us on our socials

Visit our website