[PROPOSAL #][DRAFT] V9 Lambda upgrade (with Replicated Security)

draft

---

jtremback 1 December 20, 2022, 9:07pm

V9 Lambda upgrade (with Replicated Security)

Terminology note: Interchain Security is the name for a family of protocols. The feature being discussed here is in this family, but more accurately termed “Replicated Security”. In the past it has been referred to as Interchain Security v1, or ICS, but going forward we refer to it as Replicated Security.

Changes to this proposal

This proposal went onto the governance forum in mid-December. Since that time, we have made one change to the protocol. In response to the only high-severity finding in the **Informal audit report**, and feedback from the community, we have made it so that the slashing and tombstoning of validators for offenses on consumer chains must be approved by a governance vote. This will have a **very minimal impact** on the operation and security of consumer chains while protecting the Cosmos Hub from possibility of an attack by a rogue consumer chain.

This governance gating is temporary until the Cosmos Hub is able to cryptographically verify proof of double signing in an upcoming release of Replicated Security. This does not give governance the ability to slash validators arbitrarily, but rather to approve slash packets that have already been transmitted from a consumer chain.

Summary

The Cosmos Hub is upgrading its security system with a new feature called Replicated Security. This will allow the Cosmos Hub to provide its strong security to other blockchains, which are called “consumer chains”. The cost to censor or control a consumer chain with an economic attack is the same as the cost to censor or control the Cosmos Hub itself. This means that consumer chains can benefit from the Cosmos Hub’s security without having to maintain their own validator sets.

Replicated Security works through the IBC (Inter-Blockchain Communication) protocol. Consumer chains receive periodic IBC packets containing the up-to-date validator set of the Cosmos Hub. They use this information to update their own validator sets, effectively replicating the Cosmos Hub’s validator set across all consumer chains. This means that the Cosmos Hub’s validators can validate multiple blockchains at once with the same stake.

In exchange for this service, consumer chains are expected to send a portion of their fees and inflation to the Cosmos Hub validators and delegators. These tokens will then be included as part of the Cosmos Hub’s staking rewards.

The ATOM economic zone

It is anticipated that consumer chains using Replicated Security will collaborate closely in an "ATOM economic zone". This is expected to have a snowball effect, with the Cosmos Hub securing a growing group of high-value decentralized protocols. Already, some prominent projects such as a smart-contracting platform, an AMM, several liquid staking providers and others have expressed interest in using Replicated Security from the Cosmos Hub.

Replicated Security can also be used to further the cause of "Hub minimalism". Any new features to the Hub, even if they are core to the Hub's functionality, can be launched as consumer chains. This allows the Hub to scale better and separate release cycles, enabling faster deployment of new features.

Onboarding a consumer chain

This governance proposal will not launch any consumer chains on its own. Instead, it will only add the necessary code to the Cosmos Hub to enable Replicated Security. In order to launch, each consumer chain must submit their own governance proposal to be voted on separately.

It is expected that before launch, a consumer chain will have participated in a Cosmos Hub Replicated Security testnet, conducted their own testnets, and undergone an audit by reputable auditors.

Once a consumer chain proposal passes, Cosmos Hub validators can begin running the consumer chain and receiving rewards. The chain will only start if more than ⅔ (by power) of the Cosmos Hub validators decide to run the consumer chain.

Offboarding a consumer chain

Once the consumer chain is running, validators can be slashed and jailed for consensus faults such as downtime and double signing on the consumer chain.

At any point in time, ⅓ (by power) of the Cosmos Hub validators will be able to stop running the consumer chain at once: the chain will halt, and none of them will be slashed for downtime.

The offboardings of consumer chains will have strong social norms to protect both sides, and any kind of forceful exit will only be coordinated in extreme cases such as protocol failures or attacks.

For normal cases, a separate governance proposal will be made to remove a consumer chain, which will allow Cosmos Hub validators to stop running it.

FAQs

How will the community ensure the quality of the consumer chains?

First, this proposal by itself does not start any consumer chains. Each consumer chain will need to be confirmed in a separate proposal. In other words, if you support Replicated Security but only want consumer chains that meet very high standards, it would be appropriate to use your "No" vote for the proposals of consumer chains that do not meet this standard.

Second, if more than ⅓ of the Cosmos Hub validators do not want to run a consumer chain, it will not run, regardless of how the governance vote went. This applies both to the start of the consumer chain, and continues to apply throughout its life.

For the avoidance of doubt, no validator will ever have to run, or will be slashed by a consumer chain which has not first been approved by governance, and then "accepted" by ⅔ of the validators intentionally choosing to run the consumer chain code.

Why would a Cosmos Hub validator want to run a consumer chain?

Replicated Security is a long awaited feature that will put the Cosmos Hub at the center of a constellation of valuable ATOM-aligned consumer chains. The consumer chains who will be introducing proposals to launch over the next year are some of the most highly-anticipated projects in the Cosmos space.

Replicated Security incorporates some fee-split mechanisms where a percentage of the value-captured by each consumer chain is sent to the Cosmos Hub validators and delegators.

Over time the fees may be raised as the value of being in the exclusive set of Cosmos Hub consumer chains is recognized, or perhaps lowered as validators improve their infrastructure and practices to be able to spin up new consumer chains more cheaply.

Over the long-term, Cosmos Hub validators and delegators may also consider a possible appreciation of their staking rewards as replicated security establishes itself as an important value-capture mechanism for ATOM.

In any case, governance will need to look at each consumer chain separately and decide whether the fee split makes sense for the consumer chain in question.

How should validators think about revenues and costs?

There are multiple ways a consumer chain could remunerate the Cosmos Hub validators

1. Transaction fees: By default, 25% of the consumer chain fees will be distributed to the provider chain. This number can be set differently for each consumer chain. Note that validators also have control over the minimum fee they are willing to receive.

2. Token inflation: If the consumer chain has a token, they can allocate a portion of the inflation to the Cosmos Hub validators and delegators (in other words, "continuous airdrops").

3. Application fees: If the consumer chain doesn't have a token, a percentage of the swap fees, usage fees etc. can be distributed to the provider chain as well.

Each consumer chain will be responsible for putting up a governance proposal outlining a commitment to use a combination of these revenue streams to compensate the Cosmos Hub community for the replicated security service.

On the expense side, the hardware costs of running a new chain may range from $100 to $1000 based on the chain requirements and the technical setup selected by the operators. Informal Systems will be working with validators during 2023 to analyze resource usage and recommend cost-effective validator setups.

Another important component of the expense of running a chain is staying on top of upgrades and governance. For consumer chains upgrades, Hypha Coop and Informal Systems will establish a regular and predictable cadence of upgrades to each consumer chain to minimize time spent by validators. For consumer chain governance, Cosmos Hub validators will not need to participate in governance of any consumer chains, since

they have their own governance mechanisms built.

Can the validators stop validating a consumer chain?

If it turns out that a given consumer chain is no longer worth validating because it is unreasonably taxing on validator infrastructure, or because it does not have high potential for future growth, then it can be stopped by a governance proposal.

In the worst case scenario, such a low-performing consumer chain can be stopped by ⅓+ of the validators simply turning off their nodes. As discussed above, in this scenario, no validator will be slashed for downtime.

What security problems could a malicious consumer chain cause?

The protocol design of Replicated Security currently assumes that consumer chains are audited before they are approved for launch. Reputable independent auditors are expected to conduct these audits. Before approving any consumer chains, governance voters are encouraged to review the audit findings. Auditors of consumer chains are encouraged to include a section in their reports that details the code's adherence to the correct Replicated Security protocol.

However, we have also taken the following steps to limit the damage that a malicious consumer chain could cause in several scenarios.

One potential issue is malicious slashing, where a consumer chain attempts to slash every validator on every validator on the Hub at once by falsely sending packets claiming that the validators equivocated (double signed) on the consumer chain. To prevent this, slashing for equivocation on consumer chains must additionally go through a governance process before the validator is actually slashed. This is an extra layer of safety, and will have **very minimal effects** on consumer chains (the only concrete effect is that they will need to set an IBC parameter known as the "trusting period" to 5 days). In the next version of Replicated Security, the Cosmos Hub will be able to verify equivocation evidence automatically, and we can remove the governance gating.

Another potential issue is malicious jailing, where a consumer chain attempts to jail every validator on the Hub at once by falsely sending packets claiming that the validators had downtime on the consumer chain. However, these jailing packets are throttled, so that only one percent of the Hub validator power can be jailed per hour. Combined with the fact that jailing only lasts 10 minutes, it will not be possible for a malicious consumer chain to cause anything worse than transient disruption.

It should also be noted that the parameters around downtime jailing (e.g. how long a validator can be down on a consumer chain before being slashed) cannot be modified by a consumer chain's governance. These parameters will be configured to be more lenient on consumer chains than on the Cosmos Hub.

Another potential issue is the misuse of validator keys. Validators can choose to use the same private key on both the provider and consumer chains, but this exposes them to the risk of their key being misused by a malicious consumer chain. To avoid this, validators can assign a different key for each consumer chain, which will prevent any potential misuse of their key.

Finally, the ability for Cosmos blockchains, including consumer chains, to use fully custom binaries could potentially be used to harm the underlying infrastructure. For example, a Cosmos chain binary could hypothetically erase the hard drive it was on. However, validators use virtualization technologies that allow them to run a different virtual machine for each chain, including consumer chains. This will prevent any harm

to the underlying hardware.

Overall, while malicious consumer chains pose security risks, we have implemented measures to limit the potential damage they could cause.

How was the correctness of the Replicated Security ensured?

The Cosmos Hub team at Informal Systems used a wide variety of approaches to ensure the correctness and security of the Replicated Security module. It was then audited by the Model Based Testing team at Informal, as well as several other teams.

Confidence in the correctness was increased of the ICS code through **various testing approaches**:

- Unit tests are useful for simple standalone functionality, and CRUD operations.
- **End to End tests** utilize the **IBC Testing Package**, and test functionality that is wider in scope than a unit test, but still able to be validated in-memory, i.e., code where advancing blocks would be useful, simulated handshakes, simulated packet relays, etc.
- **Differential testing** is similar to e2e tests, but they compare the system state to an expected state generated from a model implementation.
- **Integration tests** run true consumer and provider chain binaries within a docker container and are relevant to the highest level of functionality. Integration tests use queries/transactions invoked from CLI to drive and validate the code.

Worst-case scenarios circuit breakers were added to ensure the stability of the Cosmos Hub:

- **Governance gating of slashing** – Makes it so that slashing a validator for equivocation (double signing and related attacks) on a consumer chain must be ratified by Hub governance. As a result, an attacker that compromises a consumer chain cannot jail all the Cosmos Hub active validators at once and replace them with its own validator set, since the obvious fraudulent slashes will be voted down.
- **Jail packet throttling** – makes it impossible to jail more than 1% of the power on the Cosmos Hub per hour. For more details, see **github issue**.
- **Unbonding liveness** – makes it impossible for un-delegations to never complete (which would result in users never getting their staked Atoms back).

Several audits were completed with multiple ecosystem partners:

- Protocol audit performed by the Apalache team at Informal Systems
- IBC audit performed by the ibc-go team at Interchain
- Informal Systems Audits team has provided continuous security feedback, and has conducted **an audit**

An incentivized testnet was also run for 4-5 weeks (Game of Chains) and findings were analyzed.

31 Likes

Preparing for Replicated Security

Findings from Game of Chains and Beyond

---

dimiandre 2 December 21, 2022, 12:13pm

This is a no-brainer yes ❤️

7 Likes

Instafinanzas 3 December 21, 2022, 1:31pm

Excited about this!

Do you foresee other challenges for validators besides the ones explained here?

Also, probably dumb questions but is there a limit on consumer chains the hub can secure?

2 Likes

---

jtremback 4 December 21, 2022, 5:00pm

I think we've got everything on here. We're always looking for more feedback, but the main concern we've heard is infrastructure cost and time spent.

We'll be working with validators to reduce infrastructure cost of consumer chains while maintaining the same security and performance, and we'll be working with consumer chain teams to orchestrate chain upgrades in a steady and predictable cycle to reduce time spent.

3 Likes

Nickweldingdiaz 5 December 21, 2022, 5:33pm

It's basically permissioned. Which is a good thing…

ICS will bring so much value to cosmos, the validators are going to a do a good job.

It's no easy task, I can see it will be a big job to monitor all of this.

I say YES… I can't wait to see what else follows and these chains that pay fees to validators in return will be paid out to stakers I assume.

This is a GAME CHANGER!

2 Likes

VK_S16 6 December 22, 2022, 4:29am

Good proposal.

For now, that's exactly our concern as a validator. Hope we can have some sustainable solutions to this. Thank you.

1 Like

---

johnniecosmos 7 December 22, 2022, 11:26am

Thanks for yours and Informal's work on ICS and thanks for putting up this draft proposal Jehan.

2 Likes

Govmos 8 December 22, 2022, 12:30pm

> jtremback:
>
> - Transaction fees: By default, 25% of the consumer chain fees will be distributed to the provider chain. This number can be set differently for each consumer chain. Note that validators also have control over the minimum fee they are willing to receive.
> - Token inflation: If the consumer chain has a token, they can allocate a portion of the inflation to the Cosmos Hub validators and delegators (in other words, "continuous airdrops").
> - Application fees: If the consumer chain doesn't have a token, a percentage of the swap fees, usage fees etc. can be distributed to the provider chain as well.

It seems very good balance in here; We look forward for other people's feedback, but our early assumption is that this seems well crafted, with enough room to adjust on a case to case basis without introducing too much complexity in return. 👍

3 Likes

waqarmmirza 9 December 22, 2022, 1:16pm

Thank you for explaining it so well. It looks like a well-balanced proposal. But I have a few questions.

1- Can a consumer chain cause a provider chain halt in this case the Hub? if yes how can we avoid that?
2- When you say 2/3rd of validator needs to say yes it means 117 validators currently or the 2/3 of total val turnout. Because there are a few dozen Val who doesn't participate at all.
3- Validator funding should be more explained as not all of the validators are well-funded.

Thanks in advance

2 Likes

---

lexa 10 December 22, 2022, 2:18pm

> waqarmmirza:
>
> 2/3rd of validator needs to say yes

2/3 refers to 2/3 of the total staked ATOM on the Hub.

ATOMs are staked with validators, which is why we sometimes refer to it as "2/3 of validators" when it's shorthand for "validators who cumulatively hold 2/3 of the total stake".

Enabling a consumer chain requires a YES vote by governance but it also requires validators to set up a node and run a new binary - there may very well be validators who will do that work but still not participate in tokenholder governance.

3 Likes

---

waqarmmirza 11 December 22, 2022, 2:44pm

Yes, it totally makes sense, idk from where i got that.
16.88 VP of 23 validators never participated in the Governance. this means roughly 80% from ~83% of the remaining vp from 152 validators must vote yes to pass the prop. this is ambitious.

2 Likes

---

lexa 12 December 22, 2022, 2:53pm

Are you talking about governance voting or having validators choose to run the code? The quorum and passing threshold for governance votes is the same for this proposal as it is for others, so no more ambitious than any other proposal. The Hub docs were recently updated to clarify some of these governance voting concerns, so you might find them helpful: **On-Chain Proposal Process | Cosmos Hub**

For governance votes, 40% of stake must participate (voting yes, no, nwv, or abstain) to reach quorum. Once quorum is reached, if >50% of the *participating voting power* (i.e., All the stake that has cast a vote in this particular proposal) has voted YES and <33.4% has voted NWV, the proposal passes.

The 2/3 of voting power refers to having validators actually run the code, which is the same requirement as running the Hub itself! Like I said before, validators who don't participate in governance are still participating in securing the chain.

3 Likes

---

waqarmmirza 13 December 22, 2022, 4:37pm

Simply put.

Simple gov prop to onboard code > Val will start the node but the chain will only start when 2/3 VP reaches > once the chain starts any active hub validator not running any of the consumer chains will be slashed (downtime).

1 Like

---

zero_00 14 December 22, 2022, 5:33pm

*.— [**Unbonding liveness**]– makes it impossible for un-delegations to never complete (which would result in users never getting their staked Atoms back). -----
This is terrific, means delegators can lose their staked assets? could you please give us a deeper explanation of when and why this could happen?
Thanks.

1 Like

---

lexa 15 December 22, 2022, 5:49pm

> Simple gov prop to onboard code > Val will start the node but the chain will only start when 2/3 VP reaches > once the chain starts any inactive hub validator not running any of the consumer chains will be slashed (downtime).

Just a few clarifications, as I want to be sure we're on the same page about validator activity and running "any" of the consumer chains.

The following will have to happen anytime a consumer chain is proposed:

1. Simple gov prop on the Hub to onboard code, requires normal gov quorum and 'YES' threshold to pass.
2. Once passed, validators will start their nodes and the specific consumer chain will only start when 2/3 of the Hub's voting power is running the chain code.
3. Once the chain starts, any **active** Hub validator not running the specific consumer chain will be slashed for downtime.

Inactive Hub validators do not participate in producing blocks for the Hub or any consumer chain. and are thus not at risk of being slashed for downtime until they join the active set.

1 Like

---

lexa 16 December 22, 2022, 6:01pm

@zero_00

> [**Unbonding liveness**] - makes it impossible for un-delegations to never complete (which would result in users never getting their staked Atoms back).

This is saying that there *was* a worst-case scenario in which an undelegation message could be frozen and thus never complete, resulting in users being unable to unstake their ATOMS. Bad stuff, for sure.

The good news is that this is was resolved - the proposal text here says that the 'unbonding liveness' circuit breaker was added to make such a situation impossible in the future.

I can see why the double negative is confusing! Maybe best to read it as:

> [**Unbonding liveness**] - **Fixes** an issue in which an undelegation fails to complete, resulting in users never getting their staked ATOM back.

Related Github issues as I was looking into this:

- **VSCPackets should have timeout on provider**
- **Channel initialization should have a timeout**

6 Likes

---

waqarmmirza 17 December 22, 2022, 6:28pm

Thank you, there was a typo, but this is same what I said.

This leaves us with the validator funding, as mentioned it costs 100-1000 to operate a node. for the sake of argument, we say the cost is $450 for a node, at the current price it is 50 Atom.

A validator with 200K delegations and 3% commission earns ~100 Atom monthly. bottom 75 validators have less than 200K atoms staked.

How can a validator run multipole consumer chains with this maths? and theoretically, they are dependent on the consumer chain tokenomics for this funding.

1 Like

LeonoorsCryptoman 18 December 22, 2022, 8:16pm

> jtremback:
>
> This is expected to have a snowball effect, with the Cosmos Hub securing a growing group of high-value decentralized protocols.

I would like this part changed. Having the same set of validators potentially securing lots of consumer chains is still centralized. Decentralisation should only be used if it meets 3 characteristics:

- decentralisation in location (global spread)
- decentralisation in voting power (as @waqarmmirza rightfully indicates, we have a serious issue here on costs to operate validators in the lower ranks)
- decentralisation in validators

Replicated security is a serious risk imo regarding validator decentralisation; which is something we should take seriously. The barrier for new validators to join the active set will only become bigger over time. And bigger validators have more people to run the stuff, so feeling more secure for a lot of people; probably causing more centralisation of voting power. How are these things tackled?

1 Like

---

jtremback 19 December 22, 2022, 9:06pm

We can certainly take the word “decentralized” out of the proposal if a lot of people object. It’s a term that is impossible to define rigorously. For example, many Bitcoin maximalists believe that no proof of stake chain can ever be decentralized.

What we can say for certain is that all consumer chains will be just as decentralized as the Cosmos Hub. Whether or not the Cosmos Hub is currently decentralized is outside of the scope of this discussion. I think it is.

The question of whether replicated security will make the Cosmos Hub less decentralized by hurting small validators is completely valid though. This is the main concern we have heard, and it will be the Cosmos Hub team’s top priority for 2023. We will be making sure that consumer chain testnets and upgrades are as smooth and regular as possible to minimize the human workload on validators. We’ll also be working with validators to review the infrastructure cost breakdown of their setups and see how we can implement code to lower it for consumer chains.

Finally, this proposal by itself does not launch any consumer chains, it just installs the code to make replicated security possible. The question of whether a given consumer chain is worth running is best asked when that consumer chain is being proposed.

6 Likes

---

zero_00 20 December 22, 2022, 10:52pm

Thanks a lot for the fast and precise reply-

1 Like

---

waqarmmirza 21 December 23, 2022, 6:18am

If we keep ourselves in the scope of this draft proposal, we should have a concrete plan for validator funding.

I really liked that the hub team is aware of the problem and wanted to work on this thoroughly, but I am not comfortable with a proposal that talks about the problem but doesn’t give a proper solution but instead gives the timeline to solve the problem, and that solution might be unacceptable to the majority but we won’t be able to reverse replicated security and offboard multiple chains, that will be a disaster.

This might sound like a dystopian scenario but It can happen given the situation. So we should talk openly about the funding of the validators.

We need a set of rules for how the consumer chain will fund the validators.
If a consumer chain fails in funding who will bail out? the treasury?

Keep in mind the overall market condition of the industry and the timing of this proposal, if a big bitcoin mining company can go bankrupt, our beloved validator teams can go bankrupt too with the lack of funding.

Out of scope but the important point is in most of the bottom of the chain 85% of the validators are not even breakeven.

Ghazni_Stakecito 22 December 23, 2022, 12:44pm

We have been thoroughly testing ICS in Game of chains and are very much in favor of this. Its time for Cosmos Hub to get some value accrual. 💪

4 Likes

---

lexa 23 December 23, 2022, 2:26pm

Personally, I would expect that the Hub would just reject consumer chains that are not somewhat profitable and prepared to adequately compensate the Hub. It's clear that we have different risk tolerances on this (and that's fine - collegial disagreement like this is how we come to the best ideas)!

From my perspective, enabling Replicated Security doesn't produce the problem, so it's not in the scope of the proposal to fully address it. Each consumer chain that wants to come onboard will potentially produce the problem, so it's in the scope of those proposals to solve it. Especially because we're bound to have a variety of projects with very different needs and revenue expectations, so there may not be a one-size-fits-all solution.

> We need a set of rules for how the consumer chain will fund the validators.

The thing I hope we all agree on is that Hub validators deserve not only break-even compensation, but profit! You're absolutely right that we need some guidelines and social norms around it.

I've been working with the ICS team and some consumer chains to put thoughts together on this and I have an essay I'm really excited to share 🙂 I'll publish early in the New Year, but I need to take some time off for the holidays with my family 🎄

7 Likes

---

zero_00 24 December 23, 2022, 4:54pm

Enjoy the family I wish you all the best, regarding to compensation / profit what can be almost a utopia it's to be paid in stable coin instead of $Atom this could prevent sell pressure and help communities to focus on the tech Cosmos offers but not in the price.

---

waqarmmirza 25 December 23, 2022, 6:07pm

I am glad that you acknowledge that we need some social norms and guidelines. Will be happy to read your essay.

Enjoy your time with the family. Merry Christmas.

1 Like

Ertemann 26 December 27, 2022, 10:00am

Will just mention that as hub validators we share these concerns.

Validators are forced to run sidechains (at least in the current form of ICS) significantly complicating infrastructure requirements and knowledge required for all validators. If chains pass with a minimal yes vote for the on-chain governance we run the risks of not being able to start consumer chains or keep them running if the rewards are negligible. Especially validators at the bottom set will have a harder time supporting the hub if the sidechains dont bring direct value.

Less of these problems will exist in the future version of ICS where replicated security is not 1:1 with the Hub.

However, we are very excited for ICS to come to the hub after running GOC and will vote yes when the upgrade proposal comes online.

3 Likes

LeonoorsCryptoman 27 December 27, 2022, 7:03pm

Now you make me curious. Have been dying to enter the active set on the Hub (but do not have the funding yet), but this sounds like a new reason really wanting me to enter the set…

Have some nice days off and when your essay is here I will give it time to read it 🙂

Cryptopital 28 December 27, 2022, 8:16pm

It is a clear and massive yes for me as for GATA DAO Zone !
The Game of Chains challenge was very interesting and also quite a sucess !

Nice work as always !

Boisnou 29 December 28, 2022, 9:24am

Very smart ! Future of ICS will be awesome !

---

velvetmilkman 30 December 29, 2022, 4:34pm

> At any point in time, ⅓ (by power) of the Cosmos Hub validators will be able to stop running the consumer chain at once: the chain will halt, and none of them will be slashed for downtime.

- Since halting the chain does not require a vote, does this create or increase the risk of a centralized, existential threat to the consumer chain and users of its product(s)? How can Cosmos Hub reduce the level of uncertainty users and developers will face when they consider using the consumer chain's product(s)?
- Does the consumer chain return back online if it regains 2/3 validator support?
- Is there a "grace period" being considered for when this happens? It would be great if a consumer chain would continue to remain live with fewer than the full 175 Cosmos Hub validators for a short period of time as it attempts to regain 2/3 support of the Cosmos Hub validators. It would also provide the chain with a sufficient buffer in the case where it may be required to organize a smaller validator set and prepare to move towards full sovereignty.

2 Likes

---

velvetmilkman 31 December 29, 2022, 5:22pm

> Once a consumer chain proposal passes, Cosmos Hub validators can begin running the consumer chain and receiving rewards. The chain will only start if more than ⅔ (by power) of the Cosmos Hub validators decide to run the consumer chain.

- Is it possible to run a validator for a consumer chain without running infra for Cosmos Hub?
- How do validators signal they are ready to support a consumer chain? Do they simply run the current testnet until the 2/3 quorum is reached?
- What happens if fewer than 2/3 of validators are running infra for an extended period of time (say 3 months) before 2/3 validators decide to run the consumer chain? Are validators compensated for signaling earlier support? Is this a "consumer chain" problem that each team will deal with on their own?

1 Like

AnewbiZ 32 January 2, 2023, 5:09pm

Easy yes from me. ICS is one of the most bullish cases for ATOM. LFG

---

lexa 33 January 2, 2023, 8:53pm

> Since halting the chain does not require a vote

This applies to all the Cosmos chains - the chain will halt if >1/3 validators stop running. In that sense, the risk of a centralized existential threat seems no greater than it is on any other chain.

> Does the consumer chain return back online if it regains 2/3 validator support?

Yes. When a sufficient number of validators are running the binary again, it will start up.

The grace period is a curious idea, but I personally think it is outside the scope of Replicated Security. I do want to point out that a chain CAN remain live with fewer than 175 validators - so long as >2/3 of the validators (by voting power) are running the binary, the chain is life and the active validators not running it are being slashed.

I think that the norms necessary for this offboarding period are more in the off-chain communication and collaboration than in code that would allow a technical grace period for the edge case. I envision maybe a signalling proposal for removing a consumer chain followed by a grace period in which the consumer chain should be setting up its own validator set (which may very well include Hub validators who want to keep supporting their project). But that is different from remaining a consumer chain with only partial support from Hub validators.

> Is it possible to run a validator for a consumer chain without running infra for Cosmos Hub?

No. The consumer chain is leasing the full replicated security from the Hub's validator set, so all of the validators involved are also running Hub infra. A while back there was talk of a version of ICS in which there could be a partially duplicated validator set (e.g., Some Hub validators and some non-Hub validators) but that's not in the scope of Replicated Security.

1 Like

---

moyed_a41 34 January 3, 2023, 2:29am

Great proposal. I'm really looking forward what ICS & consumer chains get bring to the Hub.

Easy Yes to this proposals, but I think concerns made by @waqarmmirza is very important. Despite of few big validators, small validators won't be able to economically maintain "if" the consumer chain's payment to hub validators are not enough.
However, if consumer chains have to pay a lot to replicate security of hub, they may choose to find their own validator set because some chains may not need as much security as hub does. And it may lead to less projects considering Replicated Security.

Also, I'm curious about consumer chains' independent governance mechanism. Although its governance cannot affect the downtime slashing, I expect consumer chains' governance decision would affect hub in some degree.

- Will hub validators incentivizes to be included in consumer chain's governance?
- Is there any consumer chains that announced about their own governance mechanism?

Thanks, Happy New Year!

2 Likes

---

velvetmilkman 35 January 3, 2023, 10:00pm

> lexa:
>
> This applies to all the Cosmos chains - the chain will halt if >1/3 validators stop running. In that sense, the risk of a centralized existential threat seems no greater than it is on any other chain.

I personally believe it's a false equivalency. It's unlikely that the incentives and motivation of Cosmos Hub validators to support Consumer Chains is equal to the incentives and motivation of a validator on "any other chain" actively deciding to enter the active validator set of "any other chain."

If the incentives and motivations are not the same, it's hard to believe the existential risk of centralization is the same.

The power dynamics and incentives of the trust supplier (Cosmos Hub validators) and the trust consumer (Consumer Chains) is a different dynamic than the incentives of Cosmos Hub validators to continue to run infrastructure for the Cosmos Hub chain.

Many of these validators have very large self-delegations. For some context, 5 out of the top 10 validators on Cosmos Hub are not known for running infrastructure on multiple Cosmos chains. Of those 5, 3/10 are investment funds who self-delegate and 2/10 are exchanges that are staking on behalf of retail customers who don't self-custody. Those 5 validators currently hold 21.27% of all currently staked ATOM. As of today, it would take at least 51 validators to make up the 21.27% delegations missing without those 5 validators' support.

I recognize the ICF delegations should reduce that amount to ~17% once it's delegated, as all the delegations will be outside the top 20 validators. However this is a very large percentage for just 5 validators and I believe

it could cause some serious problems for the longevity of ICS if not properly planned and accounted for.

1 Like

---

jtremback 36 January 3, 2023, 10:12pm

There will be a strong social convention that consumer chains that are being shut down are shut down through governance, not by validators refusing to run them. That scenario is described to illustrate what might happen in a worst case scenario, not a normal case.

Ultimately, consumer chains of the Cosmos Hub are getting the Cosmos Hub staking token distribution and validator set. We think it's a very secure one and relatively decentralized, but each consumer chain will need to decide for itself.

LeonoorsCryptoman 37 January 5, 2023, 7:15pm

Decentralisation of voting power stays a threat which needs to be addressed more openly in the long run. It is something which can be beneficial at the very beginning, but can be a major disadvantage on the longer run.

So maybe ICS will create some additional awareness for it.

I also remember that there is work being done on making the (financial) investment for validators as small as possible to make this a viable feature.

1 Like

---

jtremback 38 January 5, 2023, 7:46pm

LeonoorsCryptoman - you run a validator, right? Wondering if you have some time to meet and discuss reducing the technical requirements for consumer chains.

LeonoorsCryptoman 39 January 6, 2023, 5:03pm

Yup, shall we schedule something?

---

lexa 40 January 6, 2023, 5:17pm

> **Preparing for Replicated Security**
>
> Introduction Interchain Security (ICS) is launching in 2023 and the Cosmos Hub will become a security provider after the Lambda upgrade. After having funded **Proposal #72** and **Proposal #77** from the Community Pool, the community has already signalled soft consent around the adoption of Replicated Security, but the Lambda upgrade will finalize its inclusion in the Hub. The Hub being able to offer security to new projects means accessing the upside of any projects launching on Hub-secured consumer …

My long-awaited essay on some of the considerations relevant to consumer and provider chains. Looking forward to seeing some discussion about the nuances of this dynamic!

5 Likes

---

jtremback 41 January 6, 2023, 9:44pm

I can't figure out how to message on here lol, what's your Twitter handle?

LeonoorsCryptoman 42 January 9, 2023, 7:13pm

I saw your message on Telegram, will check my agenda in the coming days (a lot going on at the moment :P)

Adriana 43 January 12, 2023, 11:46pm

Hi team, thank you so much for working on the proposal and also for giving the community the opportunity to feedback it. We, at Kalpatech, have some questions that if answered would make us understand the proposal better.

Approval and decisions to launch a consumer chains

It is mention that each new consumer chain will need to be confirmed in a separate on chain governance proposal. Meaning that the one which is accounted for is individual staking voting power.
On the other hand, it is said that if more than ⅓ of the Cosmos Hub validators do not want to run a consumer chain, it will not run, regardless of how the governance vote went. Which means that in the end, it is the validators that are using the collective delegated stake to decide on which chains to validate and not the owner of the stake.

Are we able to make this more clearly in the content of the proposal?

Revenues

It would be great if we could add the token inflation distribution to Atom Holders as being a requirement and not just an option, or by case application fees if the chain does not have a token. Atom holders expect high revenues coming from the inflation portion of the consumer chains and would be great to not leave the possibility to opt out of it.

Governance

It is mentioned that for the consumer chain governance, Cosmos Hub validators will not need to participate in governance of any consumer chains, since they have their own governance mechanisms built. That means that the voting right of the validator is being entirely canceled and the validators will just need to implement the decisions of the token holders?
This situation might create some disagreements in the way decisions and operations are being carried on and implemented. As validators are highly invested in the success of the chain and are adding resources and bandwidth to operate it, while having no say in the outcome of the chain or the decisions which are made regarding its future implementations could be seen as difficult.

Validators running consumer chains

Any consumer chain needs 2/3 validators of the cosmoshub to start and operate the chain. Do all Cosmoshub validators need to join the consumer chain once it is live as to not risk downtime, or if they decide to not join a specific chain for validation, and that chain is live, they could do so, not validate the chain and they won't be slashed for downtime?

Security problems- malicious slashing

It is said that one potential issue is the malicious slashing, in which a consumer chain sends instructions to the provider chain to unfairly slash validators. To prevent this, a "slash throttle" that limits the number of validators that can be slashed at once, reducing the potential harm to the Cosmos Hub's consensus was included. But this measure does not prevent for a malicious consumer chain to still attempt to unfairly slash a few validators. Can the slashing instructions that are coming from the consumer chain be put in "quarantine" or some sort of alert system that requires a special signing or approval? Like freeze the state to which the instruction was sent as a record and meantime investigate and approve or deny the request.

Game of chains findings and audit

Can the findings of Game of Chains be made public and how those issues have been addressed? Also it would be great to analyze the audit reports and the recommendations which were highlighted there as well.
Can the Cosmos Hub community pool fund for an additional audit report of the RS tech? I believe, considering the high stakes of the implementation we want to make sure that we have receive a sufficient amount of feedback and review and in this case having independent audit companies to be considered as well would definitely help.

2 Likes

---

jtremback 44 January 16, 2023, 4:28pm

@Adriana will respond to all of these tomorrow, thanks!

3 Likes

---

jtremback 45 January 17, 2023, 10:10pm

> **Approval and decisions to launch a consumer chains**
> It is mention that each new consumer chain will need to be confirmed in a separate on chain governance proposal. Meaning that the one which is accounted for is individual staking voting power.
> On the other hand, it is said that if more than ⅓ of the Cosmos Hub validators do not want to run a consumer chain, it will not run, regardless of how the governance vote went. Which means that in the end, it is the validators that are using the collective delegated stake to decide on which chains to validate and not the owner of the stake.
> Are we able to make this more clearly in the content of the proposal?

This is just how Cosmos governance and consensus works. For example, if an upgrade proposal passes governance but then the validators do not want to run it, it won't run. We already emphasized this dynamic more in this proposal than it is usually talked about on most proposals, leading some people to think that it's actually something special about RS, which is not the case. So personally, I would prefer not to emphasize it even more.

> **Revenues**
> It would be great if we could add the token inflation distribution to Atom Holders as being a requirement and not just an option, or by case application fees if the chain does not have a token. Atom holders expect high revenues coming from the inflation portion of the consumer chains and would be great to not leave the possibility to opt out of it.

The RS code itself does not have any way to check what kind of payments will be made to the Cosmos Hub from the consumer chains. This is something that needs to be verified by people participating in governance during the consumer chain proposal voting period. So any requirement for inflation to be at a certain level would not be a code change, but a signaling proposal. Since this is an upgrade proposal dealing exclusively with code changes, I don't believe it's the right venue for signaling. A separate signaling proposal laying out inflation requirements might be better suited for this.

Also, in general I personally think that it should be decided individually for each consumer chain.

> **Governance**
> It is mentioned that for the consumer chain governance, Cosmos Hub validators will not need to participate in governance of any consumer chains, since they have their own governance mechanisms built. That

> means that the voting right of the validator is being entirely canceled and the validators will just need to implement the decisions of the token holders?
> This situation might create some disagreements in the way decisions and operations are being carried on and implemented. As validators are highly invested in the success of the chain and are adding resources and bandwidth to operate it, while having no say in the outcome of the chain or the decisions which are made regarding its future implementations could be seen as difficult.

I think you are right that this is potentially challenging. One of our top priorities at the Informal and Hypha Cosmos Hub teams is supporting RS, and consumer chain upgrades are at the top of our list of things to facilitate and keep an eye on.

In the future, we will be upgrading RS so that malicious consumer chain code cannot harm the Hub in any way. Together with good practices around key assignment, and sandboxing of consumer chain binaries on validator hardware, this means that validators don't actually have to care that much about the content of a consumer chain upgrade from a security perspective. This is a little bit like how Ethereum validators don't care much about the content of smart contracts running there.

So, our goal for the future is that validators load up new consumer chain upgrades with doing much due diligence because no bad outcomes are possible, and things are as automated as possible. We are not quite there, but until then, we will be playing a very active role facilitating upgrades and preventing any issues.

> **Validators running consumer chains**
> Any consumer chain needs 2/3 validators of the cosmoshub to start and operate the chain. Do all Cosmoshub validators need to join the consumer chain once it is live as to not risk downtime, or if they decide to not join a specific chain for validation, and that chain is live, they could do so, not validate the chain and they won't be slashed for downtime?

Here is a good summary of why this is not secure (the subset problem): **Informal Systems — Verifiable Distributed Systems & Organizations**

That being said, we will be setting the downtime slashing window very leniently on consumer chains. Probably around 4 days by default, and maybe much longer for the first few that are launched. This means that validators will have a very large margin of error around getting their hardware up and running on a consumer chain.

> **Security problems- malicious slashing**
> It is said that one potential issue is the malicious slashing, in which a consumer chain sends instructions to the provider chain to unfairly slash validators. To prevent this, a "slash throttle" that limits the number of validators that can be slashed at once, reducing the potential harm to the Cosmos Hub's consensus was included. But this measure does not prevent for a malicious consumer chain to still attempt to unfairly slash a few validators. Can the slashing instructions that are coming from the consumer chain be put in "quarantine" or some sort of alert system that requires a special signing or approval? Like freeze the state to which the instruction was sent as a record and meantime investigate and approve or deny the request.

A consumer chain which contains malicious code that slashes a few validators unfairly will be removed immediately by the validator community and will not come back online. After this, governance proposals can

be made to compensate the victims for slashes and time jailed, which will likely not be much money anyway.

> **Game of chains findings and audit**
> Can the findings of Game of Chains be made public and how those issues have been addressed? Also it would be great to analyze the audit reports and the recommendations which were highlighted there as well. Can the Cosmos Hub community pool fund for an additional audit report of the RS tech? I believe, considering the high stakes of the implementation we want to make sure that we have receive a sufficient amount of feedback and review and in this case having independent audit companies to be considered as well would definitely help.

Simply Staking has a proposal up on the forum for a truly 3rd party audit. I support it. The Informal audit is still ongoing and will output a report in about 2 weeks. In the meantime, here are some things that they found that we have mostly already corrected: **Issues · cosmos/interchain-security · GitHub**

@lexa did we have some kind of public report or blog post on the outcomes of GoC?

1 Like

---

velvetmilkman 46 January 18, 2023, 6:48pm

> jtremback:
>
> This is just how Cosmos governance and consensus works. For example, if an upgrade proposal passes governance but then the validators do not want to run it, it won't run. We already emphasized this dynamic more in this proposal than it is usually talked about on most proposals, leading some people to think that it's actually something special about RS, which is not the case. So personally, I would prefer not to emphasize it even more.

IMHO it should be discussed more because we're talking about adding complexity and overhead to the validator operator's operations. Beside the governance mechanics being constructed similarly, a validator operator supporting an upgrade and a validator operator spinning up additional infrastructure and increasing overhead to support a new chain is not an apples to apples comparison.

In a bear market, like the one we're in right now, economic and financial feasibility of supporting numerous consumer chains should be given greater consideration. We are no longer operating from a place of abundance.

It's not clear that incentives between delegators and delegates are aligned. ATOM stakers are incentivized to add consumer chains and potentially earn additional rewards. Many will choose the lowest commission validator. It's unclear whether validator operators' support of consumer chains will be profitable (or whether delegators even care).

1 Like

saint.Ericus 47 January 19, 2023, 11:46am

Hey everyone,

Trying to figure out how much ICS costs would actually be for new consumer chains, and would appreciate any clarifications you're able to give re my back-of-the-envelope calculations below.

A figure I've heard being thrown around is roughly 600-800 dollars per month for validators, times 175 validators. In addition to that, on top of the rewards coming from consumer chains the validators get an average fee of around 10% (meaning we'll have to multiply the results by 10 to get the revenue needed to cover such costs).

The result would look something like this:
$600 x 175 validators x 12 months x 10 = $12.6 million per year
$800 x 175 x 12 x 10 = $16.8 million per year

Although this does not consider the weight of different validators, these figures are quite extraordinary, and surely cannot be correct? Hard to see new chains being able to cover this kind of amount, especially so during a bear market like this. Or am I missing something?

Further, I'm wondering whether or not there is a normal investment risk for validators and the Hub (so if the project goes badly, the validators just lose money and vice versa) or if there are any requirements about what a consumer chain should provide in terms of value to the Hub in order to join Replicated Security?

Hope that makes sense, and again, I'm grateful for any light that can be shed on this matter.

3 Likes

LanreIge1 48 January 19, 2023, 1:10pm

Great post and excited about Replicated Security! What is the current timeline for this to be submitted as an on-chain vote/how long does this current consultation period last?

1 Like

BIN 49 January 20, 2023, 6:51am

Hi, thank you for the post.
I remember that GoC, unfortunately, ended without testing the slash feature, because the provider chain stopped as soon as the Slasher chain started sending slash packets. Was there any update on this after GoC?

---

lexa 50 January 20, 2023, 3:04pm

@jtremback and @Adriana - we are working on putting together a report on identified bugs and how they're being fixed (or have been fixed) for the v9 mainnet release. I'll link it here when we're done.

@BIN

Correct - GoC ended before this feature was fully tested. The slash rate throttling will be the first thing we test on the persistent testnet (aiming to launch next week).

We won't be moving on-chain for mainnet until it's tested and resolved.

@LanreIge1

We need to get v8 out first, and that will take at least two weeks (voting period!) from when it goes on chain. We also need to finish testing the slash rate throttle, as I mentioned. At the very earliest, we could be on-chain the week of February 6.

3 Likes

LanreIge1 51 January 20, 2023, 3:30pm

That makes sense, thanks for the response and all the work.

1 Like

BuilderBot 52 January 28, 2023, 4:07pm

> jtremback:
>
> Once a consumer chain proposal passes, Cosmos Hub validators can begin running the consumer chain and receiving rewards. The chain will only start if more than ⅔ (by power) of the Cosmos Hub validators decide to run the consumer chain.

Is it 2/3 of the validator set only or staked ATOM?

LeonoorsCryptoman 53 January 29, 2023, 6:59pm

Voting power based. So 2/3 of the total voting power (thus staked ATOM)

1 Like

BuilderBot 54 January 29, 2023, 8:34pm

(post deleted by author)

BuilderBot 55 January 29, 2023, 8:35pm

Thanks!
How long is the voting period for such proposal?
And how long it the “preparation” period, so validators can set up the consumer chain nodes?

---

lexa 56 January 30, 2023, 4:37pm

Same parameters as other governance proposals - 2 week voting period.

The ‘preparation period’ lasts as long as it takes for 2/3 of the set to bring nodes online, since there is no penalty until the chain is live. To the best of my knowledge, there’s no time-based parameter for how long validators have to come online.

---

jtremback 57 February 1, 2023, 4:14am

There is a “spawn time” in the replicated security proposal. The consumer chain can start after this time passes. So an extra preparation time could be built in by setting the spawn time to some time after the end of the voting period.

1 Like

---

jtremback 58 February 1, 2023, 4:16am

Hi everyone, we’ve decided to update RS to make some forms of slashing for offenses on consumer chains less automated in this first release to ensure the safety of the Hub. You can read about it here: **Slashing updates in replicated security**

This should not have any effect on the safety or liveness of consumer chains.

6 Likes

Hush 59 February 1, 2023, 7:08pm

@jtremback
I thought this upgrade was supposed to include the Liquid Staking Module. Was the LSM cut from the roadmap or pushed down the road?

Hush 60 February 1, 2023, 7:14pm

Can anyone tell me why Inter-chain Security was changed to Replicated security? The name may be a better descriptor of the mechanism, however the change causes confusion? Who signed off on the name change and how was it justified?

JD-Lorax 61 February 1, 2023, 8:51pm

Jehan's note in the post explains the change in terminology.

> jtremback:
>
> Terminology note: Interchain Security is the name for a family of protocols. The feature being discussed here is in this family, but more accurately termed "Replicated Security". In the past it has been referred to as Interchain Security v1, or ICS, but in this document we will refer to it as Replicated Security.

"ICS v1" requires the full Cosmos Hub validator set (or at least more than 2/3). For each Consumer Chain launched the Cosmos Hub validator set is replicated in full to run that chain. Hence Replicated Security. I don't know who signed off or what the deliberation process was. While it may be confusing to the public initially Replicated Security is arguably more correct to explain how the system works.

This Informal Systems **blog post** that compares Replicated Security and Mesh Security is helpful to understand what is meant by "Interchain Security is the name for a family of protocols."

1 Like

---

jtremback 62 February 1, 2023, 10:13pm

It does not include the Liquid Staking Module. There are several reasons for this.

First, we drastically cut down the release late last year to focus purely on shipping Replicated Security. I think this was the right choice.

Second, the LSM does not actually enable liquid staking. All it does is make it so that delegators can transfer their stake to liquid staking providers without having to wait to unbond their coins, potentially making adoption of liquid staking quicker. Liquid staking works without the LSM.

We will have to see how much community demand there is for the LSM to know how to prioritize it in upcoming releases.

3 Likes

---

jtremback 63 February 1, 2023, 10:16pm

We had been using terminology like “v1, v2, v3” to describe various types of Interchain Security, but this is not a great naming practice and was getting confusing. We are going to use descriptive names from now on, such as “Replicated Security”, “Opt-in Security” and “Mesh Security”.

We honestly should have cleaned up the naming earlier, but we figured it’s better late than never. Sorry for any confusion.

2 Likes

LeonoorsCryptoman 64 February 2, 2023, 7:51pm

> We will have to see how much community demand there is for the LSM to know how to prioritize it in upcoming releases.

Difficult part here is a bit how to measure this. What is “enough demand”?
And is that not a chicken-egg story? Because I can imagine a lot of people hold back on liquid staking their assets, due to the unbonding period and the loss of APR in that time period. So if funds can be moved freely adoption might drastically increase for LSDs.

---

lexa 65 February 8, 2023, 3:27pm

A few respondents have asked about bugs found during Game of Chains and during the Replicated Security persistent testnet. I've compiled a list with links out to issues and commentary on Github, for the more technically inclined.

> **Findings from Game of Chains and Beyond**
>
> Introduction Game of Chains has wrapped up and we're excited to present the results of approximately two months of testing on the technology behind Replicated Security. The findings from Game of Chains are the result of 90 validator teams and many core team members working together to stress-test the code behind Interchain Security. Many testing methods (model-based testing, code audits, etc) require the dev team to imagine all the things that could go wrong, but there can still be a big gap b…

---

tom 66 February 8, 2023, 4:15pm

maybe it would also break the ICS (Interchain Standards) acronym. x)

GitHub - datachainlab/ics: Interchain Standards (ICS) for the Cosmos network...

Interchain Standards (ICS) for the Cosmos network & interchain ecosystem. - GitHub - datachainlab/ics: Interchain Standards (ICS) for the Cosmos network & interchain ecosystem.

1 Like

---

santinb 67 February 14, 2023, 11:19am

This proposal is a draft and we will be modifying and clarifying it according to feedback received here before putting it on chain.

---

effortcapital 69 February 14, 2023, 3:48pm

from a timing perspective, when can we expect the prop to be on-chain? Doesn't look like there's much more additional feedback since this draft has been up for nearly 2 months

1 Like

---

jtremback 70 February 14, 2023, 8:45pm

We are just dealing with some release issues. Was supposed to go live tomorrow, might be pushed to Thursday or beyond if we are unlucky.

2 Likes

BuilderBot 71 February 15, 2023, 2:33pm

I still consider the fact that validators cannot opt-out as a major risk for institutional adoption as mentioned in this thread **Preparing for Replicated Security - #29 by BuilderBot**.

Am I the only one who sees an issue here? Ofc, if institutional adoption is not the goal then please ignore it.

In short, what if a consumer chain token can be classified as a security? Custodial stakers or stakers operating in a similar legal environment might be forced to exit the Cosmos Hub then.

Jcook_14 72 February 16, 2023, 11:42pm

I would say that there is a general opt-out in this situation. If a consumer chain token is deemed a security, and institutional investment feels threatened that they'll have to exit the system due to receiving a tokenized security as a reward. We as a community have the general ability, and right to vote the chain in question, out of ICS. The Governance gate works both ways.

1 Like