

Sup.

I wanted to take the time to discuss a new important feature we're adding in the 1.9 upgrade - The IBC emergency button.

The point of this feature is that in the interconnected ecosystem, where funds can be passed between chains without permissions or limits in the event of a hack, we - as an ecosystem - may want the ability to contain a security event to give responders time for investigation and remediation.

One of the most important things you can do in case of a breach that causes (or can cause) a loss of funds is to contain the event. That means limit the attack surface and mobility (i.e. where they can go with their funds post-exploitation).

For example, imagine Osmosis is hacked. To try and "launder" the stolen tokens, the attacker may choose to transfer them to Secret Network, swap them on Blizzard to axelarETH and escape to some Mixer on Ethereum.

Another scenario is simply a bug in IBC - imagine a bug with the light-client where you could fake transfer of funds and mint them on another chain. If we cannot turn off IBC, we cannot stop exploitation (relayers are permissionless, so a sophisticated attacker can run their own relayer).

While decentralization is a core value of the network, we think that the ability to respond to ecosystem-critical events is important. That's why we came up with the emergency stop button for IBC.

The emergency button feature is implemented as an IBC middleware, which can halt incoming and outgoing messages from any of our supported IBC stacks (transfer/compute/ICA/etc) for all IBC channels (basically all-or-nothing).

It contains two core attributes -

1. The status of the switch: On/Off
2. The admin that can toggle the switch

The admin is an address that is set by governance. It defaults to no address, so there has to be governance approval for the feature to be enabled.

The admin address can and should be a multisig, comprised of core network stakeholders across multiple time zones to ensure that there is always a response available. In the future, this address can also be used by a dedicated response team.

Lastly, the switch itself can also be toggled by governance, though this is more fitting for turning IBC back on after an event concluded.

While the emergency button can definitely be improved on, we think it's a good first start in thinking about security in an interconnected blockchain space.

We wanted to take this chance to gather the community's thoughts on this design, suggestions for improvement or general feedback.

Best,

Cash