Centralization risks and mitigation

Risk: Obol hosting the relay infrastructure

Mitigation : Self-host a relay

One of the risks associated with Obol hosting theLibP2P relays infrastructure allowing peer discovery is that if Obol-hosted relays go down, peers won't be able to discover each other and perform the DKG. To mitigate this risk, external organizations and node operators can consider self-hosting a relay. This way, if Obol's relays go down, the clusters can still operate through other relays in the network. Ensure that all nodes in the cluster use the same relays, or they will not be able to find each other if they are connected to different relays.

The following non-Obol entities run relays that you can consider adding to your cluster (you can have more than one per cluster, see the--p2p-relays flag ofcharon run):

Entity Relay URL DSRV https://charon-relay.dsrvlabs.dev Infstones https://obol-relay.infstones.com:3640/ Hashquark https://relay-2.prod-relay.721.land/ Figment https://relay-1.obol.figment.io/ Node Guardians https://obol-relay.nodeguardians.io/

Risk: Obol being able to update Charon code

Mitigation : Pin specific docker versions or compile from source on a trusted commit

Another risk associated with Obol is the Labs team having the ability to update theCharon code used by node operators within DV clusters, which could introduce vulnerabilities or malicious code. To mitigate this risk, operators can consider pinning specific versions of the Docker image or git repo that have beenthoroughly tested and accepted by the network. This would ensure that any updates are carefully vetted and reviewed by the community, and only introduced into a running cluster gradually. The labs team will strive to communicate the security or operational impact any charon update entails, giving operators the chance to decide whether they want potential performance or quality of experience improvements, or whether they remain on a trusted version for longer.

Risk: Obol hosting the DV Launchpad

Mitigation : Usecreate cluster orcreate dkg locally and distribute the files manually

Hosting the first Charon frontend, theDV Launchpad , on a centralized server could create a single point of failure, as users would have to rely on Obol's server to access the protocol. This could limit the decentralization of the protocol and could make it vulnerable to attacks or downtime. Obol hosting the launchpad on a decentralized network, such as IPFS is a first step but not enough. This is why the Charon code is open-source and contains a CLI interface to interact with the protocol locally.

To mitigate the risk of launchpad failure, consider using thecreate cluster orcreate dkg commands locally and distributing the key shares files manually.

Risk: Obol going bust/rogue

Mitigation : Use key recovery

The final centralization risk associated with Obol is the possibility of the company going bankrupt or acting maliciously, which would lead to a loss of control over the network and potentially cause damage to the ecosystem. To mitigate this risk, Obol has implemented a key recovery mechanism. This would allow the clusters to continue operating and to retrieve full private keys even if Obol is no longer able to provide support.

A guide to recombine key shares into a single private key can be accessedhere . Edit this page Previous Errors & Resolutions Next Handling DKG failure