Security

RPC nodes

The IPFS build utilizes non-secret environment variables since all IPFS content must be accessible to anyone. Therefore, the widget uses public RPC nodes to serve RPC requests. Users are explicitly notified about this fact in the UI, allowing them an option to specify necessary RPC nodes on the settings page. RPC nodes setup will be stored in a browser's localStorage and used for subsequent visits to the same IPFS gateway.

Possible localStorage leak

warning The information below might severely affect your experience with IPFS applications. Lido widgets use your browser's localStorage to store some UI settings and RPC nodes urls. If you are using an IPFS gateway, which is referencing CID hash as a part of the URL path (e.g.,{GATEWAY_DOMAIN}/ipfs/{HASH}), rather than the subdomain (e.g., {HASH}.{GATEWAY}), then other websites accessed from the same IPFS gateway can potentially view or edit your settings, because localStorage stays the same for the same domain.

To avoid this possibility, it is suggested to use IPFS gateway URL, attached to the IPFS release description, see instructions . The offered gateway uses subdomain format.

Routing

Due to IPFS gateways not automatically serving/index.html as expected by many single-page applications, the Lido Interface uses a hash-based routing. Edit this page Previous Release Flow Next Hash verification