Browser access: PIPE vs. IPFS

Browser nodes are the most user-friendly way to connect to decentralized storage networks, but this has technical limitations. These can be addressed by using a gateway, but gateways come with their own limitations.

Via a browser, users can easily connect to storage networks. Browsers, however, require that communication be encrypted via HTTPS to prevent data from being leaked or altered. HTTPS encrypts connections with the SSL/TLS protocol, making it impossible for an attacker to steal data.

Decentralized storage protocols are already encrypted, but browsers don't know this and only accept SSL/TLS. Gateway systems allow users to enter a decentralized network through a browser with all subsequent requests encrypted. However, their scalability is limited because they forward all browser traffic, becoming a bottleneck that reduces a decentralized network openness.

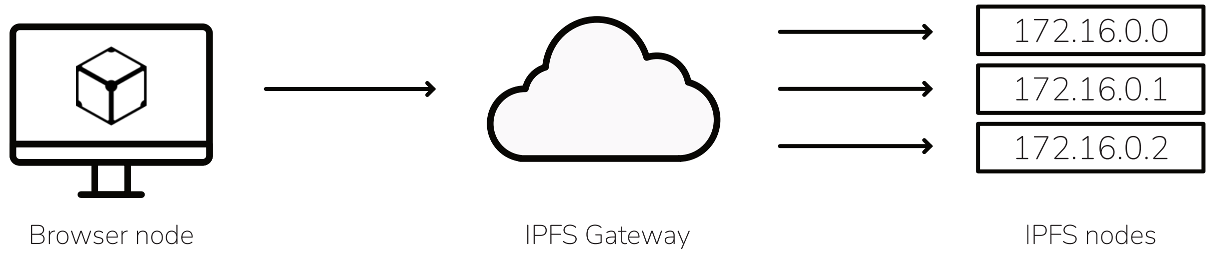
TangleHUB's team developed a fully automated, novel method of equipping every browser node in the PIPE network with full TLS capacity.

This two-pager compares IPFS and PIPE gateways and explains why PIPE is more decentralized. What's needed for a browser to securely access a network is a valid TLS/SSL certificate and a domain name somewhere in the process. PIPE provides direct network access to all browser nodes, while IPFS uses gateways.

IPFS Gateway

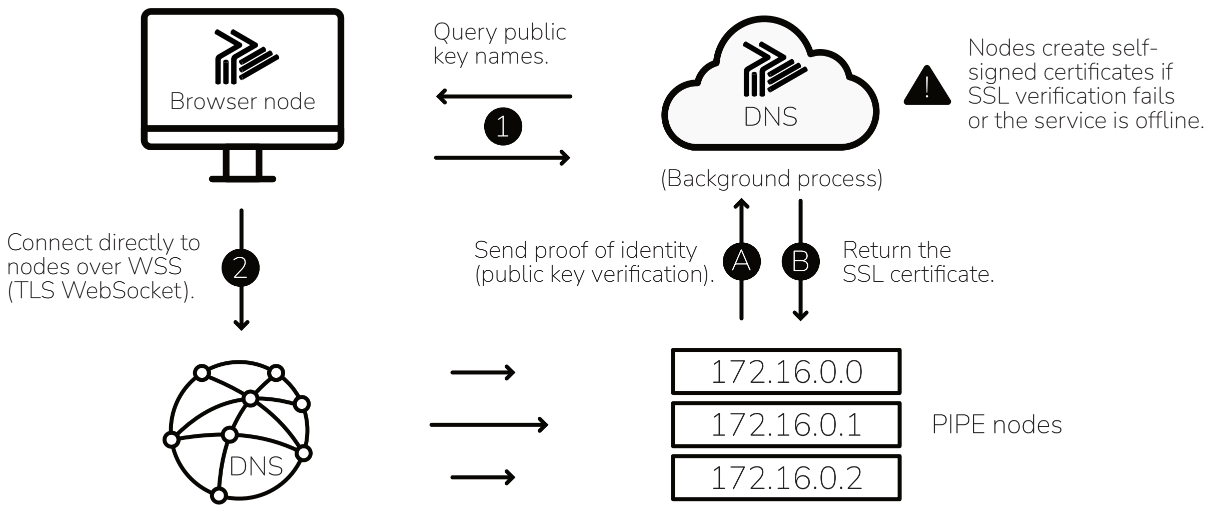
In order for IPFS to connect to browsers, various SSL/TLS secured gateway nodes forward traffic to the network. Browser nodes rely on such gateways for uptime, or they must host their own hard-to-run SSL/TLS gateway nodes.

This is a straightforward model that creates a bottleneck because gateways forward all browser traffic. Due to the volume of throughput, proper incentives are also required. Together, this increases the costs and centralization.



PIPE DNS Manager

PIPE DNS Manager links every browser node's PIPE public key to a valid subdomain under TangleHUB.eu and provides an SSL certificate. Because this open-source tool connects PIPE browser nodes to the network automatically, fast, and for free, it's fair to claim this is more decentralized than IPFS Gateways. While the process is more complex, users will not notice because it only takes seconds and is handled in the background. It also gives more reliable network access because every PIPE node is directly accessible from the browser.


Browser node
Query public key names.
1
DNS
(Background process)
!
Nodes create self-signed certificates if SSL verification fails or the service is offline.
Connect directly to nodes over WSS (TLS WebSocket).
2
Send proof of identity (public key verification).
A
B
Return the SSL certificate.
DNS
172.16.0.0
172.16.0.1
172.16.0.2
PIPE nodes

DNS Manager reliability

- DNS time to live (TTL) is set to 7 days, so linked IP addresses are cached when it is down.
- SSL certificates last 90 days. Because of this, a node only needs to connect to the DNS manager to renew every 90 days. Now uptime for TangleHUB is even less of an issue.
- DNS Manager is open-source and easy to configure, so browser access doesn't rely only on TangleHUB. Running a DNS manager requires a domain and technical knowledge. This takes 30 minutes and costs $10/year.
- Even if everything above fails, it will only affect browsers, as native PIPE nodes won't use TLS certificates. For browsers, self-signed SSL certificates are a fallback, so users may be warned but still be able to connect.

Considerations

Browser nodes are independent of the DNS manager. However, upon first boot, it connects to this centralized service (TangleHUB or a community node), and again every 90 days thereafter.

This may appear centralized, but keep in mind that it results in no gateway nodes, no forwarded traffic, and a completely decentralized network during the 90-day window, whereas IPFS always connects through some kind of gateway when you use a web browser.