FORCE
NETWORK

Introducing a new internet where everything can be private, everyone can be anonymous, and nothing can be censored

What is the Force Network?

The Force Network is intended to be a large-scale, decentralized network where participants are encouraged to provide and consume a broad range of network services in a trustless, private, and secure way.

The Force Network is capable of anonymizing any network protocol or service (e.g. internet, gaming, streaming, etc).

Why is the Force Network so Flexible?

The Force Network allows anyone to contract a wide variety of network node 'building blocks' in order to provide anonymous network services with any protocol(s) they would like to offer. This flexibility also allows the creation of services that wrap the data with any other networking protocols for additional privacy. This means an outside observer could not even tell you are using the Force Network. Privacy on both ends is increasingly important in a world where governments routinely spy on their citizens, platforms collect personal information to resell, and content hosts face direct legal consequences even for user-generated content

Data on FOR

Circulating Supply:	121,548,338 FOR
Max Supply:	200,000,000 FOR
Masternode Stake:	500,000 FOR

Exchange Listings

Crypto-bridge
Stocks.Exchange
New Exchanges coming soon

Potential Use Cases

- Maintaining privacy and anonymity even from Internet Service Providers
- Secure, zero-knowledge, and enforced encryption of e-mail and messaging
- Distributing the hosting load of a popular video stream while maintaining anonymity
- Hosting a video game server where the hosts IP cannot be discovered

Relevant Links

Website
White Paper
Discord Channel
Telegram Group
Reddit

What Makes the Force Network Unique?

Decentralized Scalable Network Services Solution

Will support HTTP/HTTPs initially, and is expandable to support any network protocol such as IPFS, DVPN, LAN gaming, E-mail, secure messaging, media streaming, and more

Totally Anonymous

The client's IP is never revealed to the payment node or content server, and vice versa. Data cannot be traced, correlated, or deciphered by any intermediary due to multi-encryption

Censorship-Resistant Network

Content hosted using the Force Network is resistant to censorship because the IP address of the content host is never directly revealed

Intelligent routing ensures scalability, resilience, and predictable performance

Node health information allows payment nodes to dynamically generate the best network paths and automatically adjust them if necessary. Approximate geolocation is optionally available to minimize latency

Intelligent Network Incentivization Model

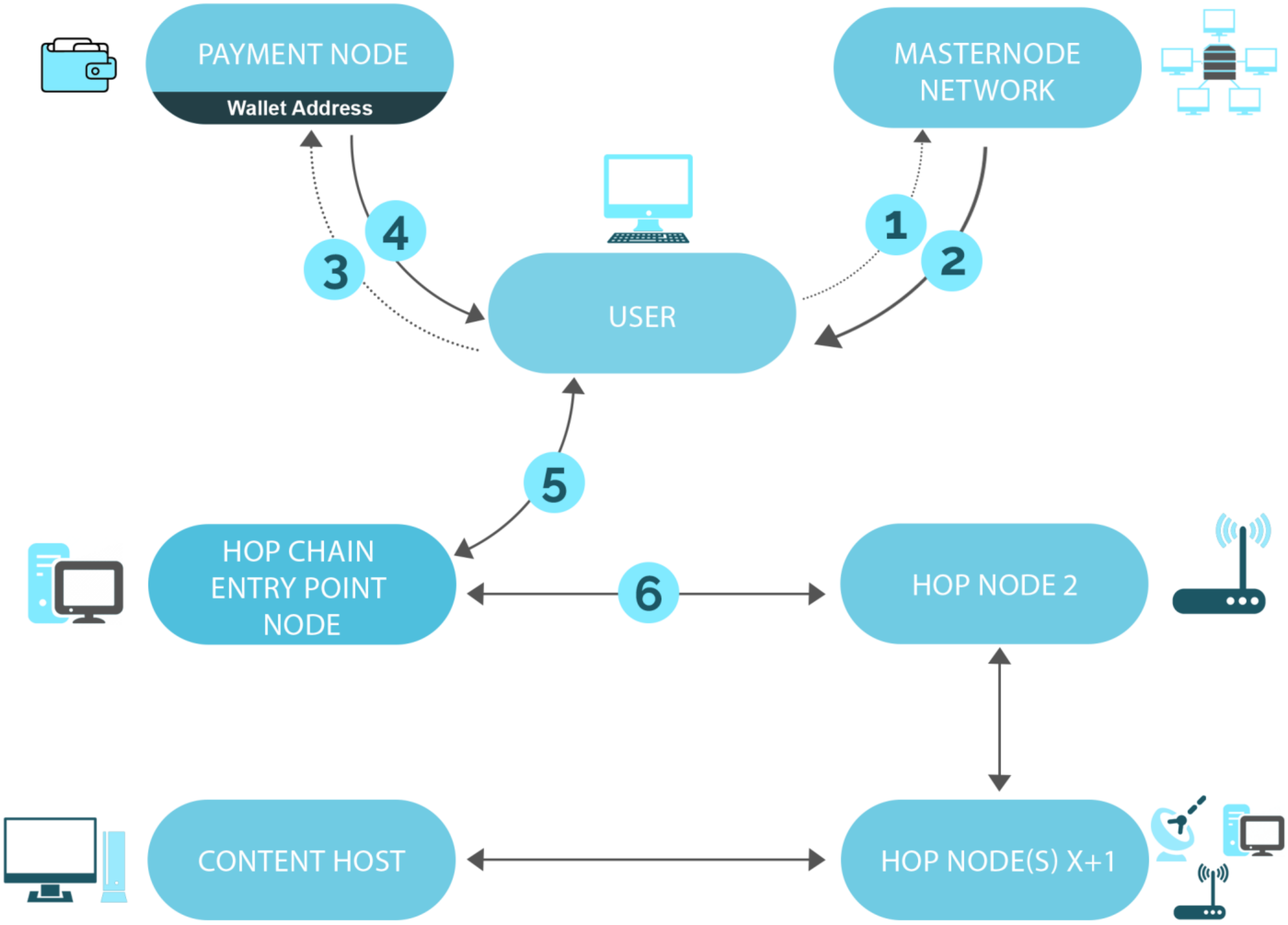
Force tokens are used to ensure a secure, resilient, and stable network. Token transactions are used to pay for network services, reward nodes, and to exchange authentication keys & IP addresses when necessary

Automated Pricing and Revenue Capability

Dynamic Service Pricing (DSP) ensures demand is met at the best possible price. Transparent service pricing allows nodes to optimally adjust offered services in order to maximize revenue

Force Network Overview

A simplified example of accessing content anonymously



1. User requests the public list of services from the closest masternode using any web browser

2. The masternode returns the wallet address of the payment node responsible for setting up the service that the user requests

3. User sends Force tokens to the payment node's wallet. This triggers the payment node to contract a chain of nodes which will anonymously forward data up and down the chain

4. Payment node sends the entry-point node IP address to the user along with keys to multi-encrypt the data so each hop can only decrypt one stage

5. User can now send and receive multi-encrypted data from the entry-point node IP as if it was the final destination

6. Requests are forwarded along the chain, with each hop decrypting one stage, and the content host decrypting it the final time. Responses are also multi-encrypted and forwarded in reverse order along the chain back to the user