D-Net Working Standard

Haoran S. Diao

December 21, 2017

Abstract

Present concerns with censorship and consolidation on the internet stem from the centralized nature of routing and address/domain registries. Control of DNS servers is a common tactic by nation-state level actors to censor content. *D-Net* Is a proposed level 3 standard that allows for decentralized and semi-trustless domain and routing records using blockchains, In turn giving rise to sender blind packet routing.

1 Global Domain Records

2 Network Topography and Routing

2.1 Nodes and Clusters

D-Net Nodes are defined as any device capable of transmitting a packet, while clusters are groups of nodes with low enough latency between them to sync up a local routing table. Clusters exist on multiple levels, with the lowest level clusters, *Level 0 Clusters*, consisting of nodes. Above those are *Level 1 Clusters* consisting of Level 0 Clusters and so on until a Level n Cluster containing all nodes on the network. A cluster/node may have multiple parent clusters.

Membership in a node is based on a simple ¿50% consensus of existing members, and periodic addition of *Sync Records* unto the Cluster Record.

2.2 Node edges and Node edge records

A node edge is any collection allowing two nodes to transfer packets. It does not matter if this edge is acheived through an intermediary, because for routing purposes, edge choice is determined by verified latency and packet loss statistics in the Cluster Record.

3 Cluster Records

Each Cluster contains inside of it a local, small block size blockchain for storing edge records and arriving at consensus. It is expected that nodes mine themselves the blocks that contain the records they publish. However, low power

nodes may arrange out of band to have other nodes mine the blocks of their records for them. Records may take up more than one block, and consist of a record body, as well as the signed hash of the body using the node signature of the publishing node.Types of records include:

- Edge Announcement
- Edge Agreement
- Edge Verification
- New Member Proposal
- Join/Leave Parent Cluster Proposal
- Proposal Vote
- Sync Record

3.1 Edge Announcement Records

When a node wishes to announce that an edge exists between it and another node either in this cluster or a neighboring cluster, it must publish a *Edge Announcement Record* into the cluster record. This record is only considered valid when the corresponding node consents by publishing an edge agreement record.

3.2 Edge Agreement Records

For nodes both on the same network, the consenting node merely publishes an agreement record, consisting of the same body as the announcement record, and the signed hash by the node signature of the second node. For nodes on seperate clusters, each node publishes an announcement record in their respective clusters, then send to eachother the bodies of these records. The two nodes then exchange signatures for the other node to publish in their on clusters.

3.3 Edge Verification

To verify the reliability of edge records, other nodes in a cluster are required to initiate a verification protocol described below. The protocol requires that all nodes store for higher an amount of time longer than the highest global roundtrip, the hash of all packets going through it.

Node A is the node doing the verification while *Node B* is the node with a record announcing a connection with *Node C*.

- Node A sends a series of packets to Node

Since by definition, clusters have to be small enough to practically sync the routing blockchain, nodes in a cluster have the same routing information, and when using determinalistic routing algorithms should come to the same routing pathes.