DNS Optimization
+
IPFS

robert@nic.ar

DNS problems.
part 1: distribution of zones to auth name servers

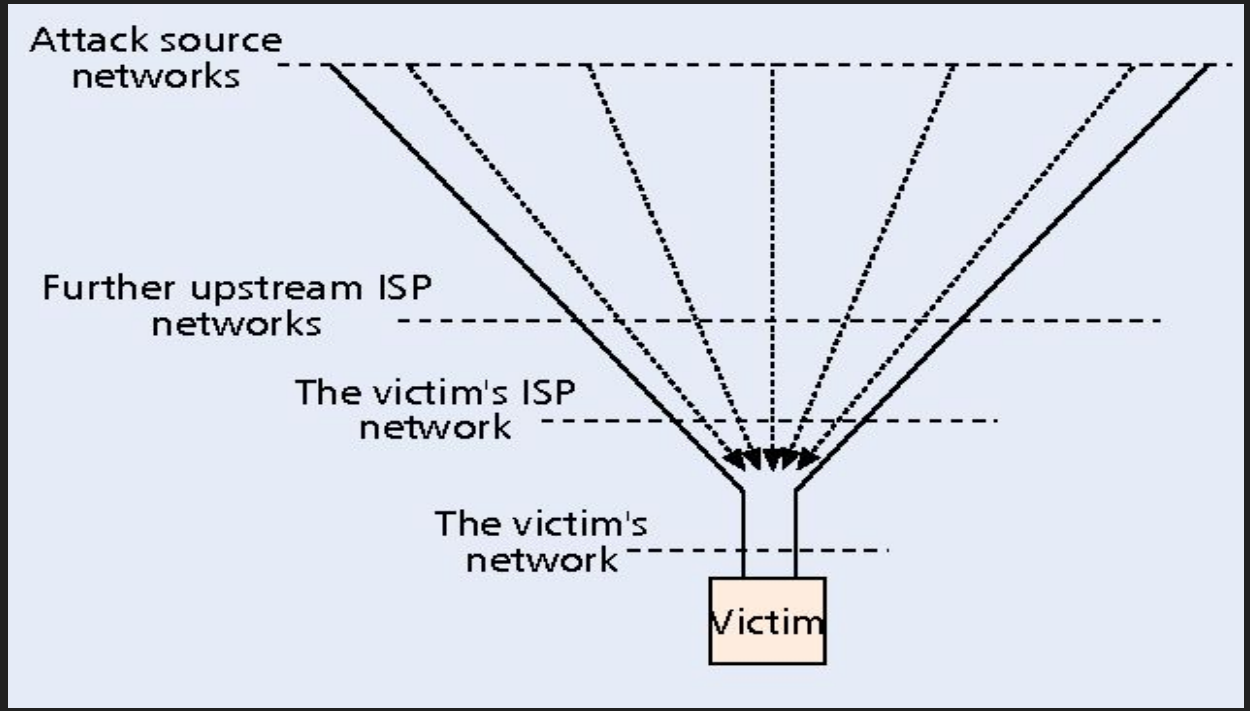
Easy to DDOS masters

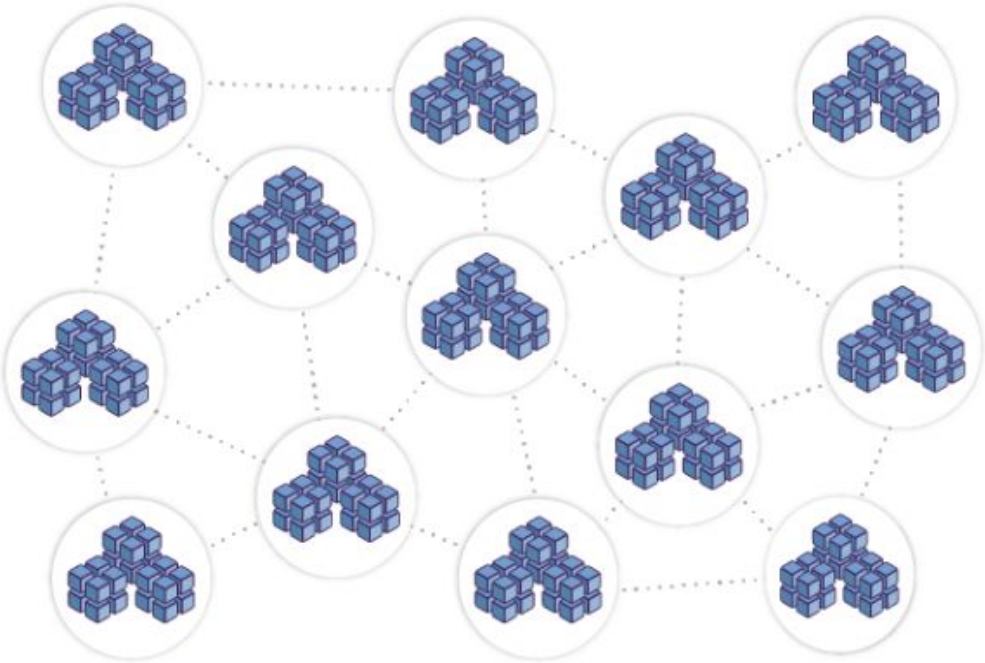
Easy to guess zone origin network

Few (hidden) masters

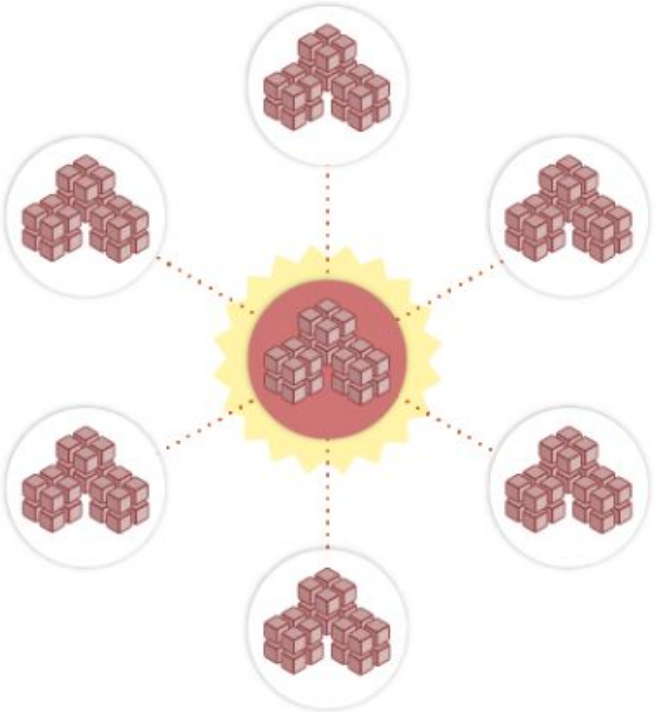
(part 2 will not be today: lookups using ipfs/p2p)

DDOS


Attack source networks
Further upstream ISP networks
The victim's ISP network
The victim's network
Victim



Red distribuida



Red centralizada

go-ipfs

made by Protocol Labs | project IPFS | freenode #ipfs | standard-readme OK | godoc reference | FAILED

What is IPFS?

IPFS is a global, versioned, peer-to-peer filesystem. It combines good ideas from Git, BitTorrent, Kademlia, SFS, and the Web. It is like a single bittorrent swarm, exchanging git objects. IPFS provides an interface as simple as the HTTP web, but with permanence built in. You can also mount the world at /ipfs.

For more info see: https://github.com/ipfs/ipfs.

Docker Pull Command

```
docker pull ipfs/go-ipfs
```

Owner

ipfs

Source Repository

Github
ipfs/go-ipfs

Your file, and all of the **blocks within it**, is given a **unique fingerprint** called a **cryptographic hash**.

IPFS **removes duplications** across the network.

Each **network node** stores only content it is interested in, plus some indexing information that helps figure out which node is storing what.

When you **look up a file** to view or download, you're asking the network to find the nodes that are storing the content behind that file's hash.

¿Qué es Blockchain?

Blockchain es una tecnología diseñada para administrar un registro de datos online, caracterizada por ser transparente y prácticamente incorruptible.

¿Cómo funciona?

A grandes rasgos, Blockchain se puede pensar como un libro contable, una bitácora o una base de datos donde solo se puede ingresar entradas nuevas y donde todas las existentes no se pueden modificar ni eliminar. Esas entradas, llamadas transacciones, se agrupan en bloques que se van agregando, sucesivamente, al registro en forma de cadena secuencial, cada uno de ellos relacionado necesariamente con el anterior.

En ese esquema, si quisiéramos corregir información ya registrada, solo lo podemos hacer mediante el agregado de nueva información. Los datos originales siempre van a permanecer y pueden ser fiscalizados en cualquier momento.

```
// 20190401 Robert Martin-Legene <robert@nic.ar>
// Stamper
// vim:filetype=javascript

pragma solidity ^0.5.2;

contract Stamper {
    struct          stamp {
        uint256         object;
        address         stamper;
        uint256         blockno;
    }
    stamp[]         stamplist;

    // Mapping de objects stampeados a la stamplist
    mapping ( uint256 => uint256[] )  hashobjects;

    // Mapping de cuentas que stampean (stampers) a la stamplist
    mapping ( address => uint256[] )  hashstampers;

    constructor() public {
        // No queremos que haya stamps asociados a la posicion 0 (== false)
        // entonces guardamos ahi informacion de quien creo el SC y en que bloque
        stamplist.push( stamp( 0, msg.sender, block.number) );
    }

    // Stampear una lista de objects (hashes)
    function put( uint256[] memory objectlist ) public {
        uint256     i           =   0;
        uint256     max         =   objectlist.length;
        while ( i<max )
        {
            uint256     h       =   objectlist[i];
                    // stamplist.push devuelve la longitud, restamos 1 para usar como indice
            uint256     idx     =   stamplist.push( stamp( h, msg.sender, block.number ) ) - 1;
            hashobjects[h].push( idx );
            hashstampers[msg.sender].push( idx );
```

rlegene/bfanode ★

By rlegene • Updated 10 days ago

The quest to get more uniform BFA nodes

Container

Manage Repository

Pulls 31

Overview | Tags

Running Dockers on Ubuntu/Debian hosts? Read https://docs.docker.com/install/linux/linux-postinstall/#your-kernel-does-not-support-cgroup-swap-limit-capabilities

To run your own bfanode, run: docker run -d --name bfanode --memory 4g -p 30303 -p 127.0.0.1:8545 -p 127.0.0.1:8546 --restart=unless-stopped rlegene/bfanode

Port 30303 will be reachable from the world. 8545-8546 only from localhost or from hosts you --link it to.

It should take a few hours to synchronize. You can monitor the import of blocks with: docker exec bfanode bfalog.sh

By default the node will have no account associated with it.

Docker Pull Command

```
docker pull rlegene/bfanode
```

Owner

rlegene

Terminal - bfa@cloud-j1: ~

File Edit View Terminal Tabs Help

```
#!/usr/bin/node

"use strict"

const   BigNumber   =   require('bignumber.js');
const   Libbfa      =   require( process.env.BFAHOME + '/bin/libbfa.js');
var     bfa         =   new Libbfa();
var     web3        =   bfa.newweb3();
var     Distillery  =   bfa.contract( web3, 'Distillery' );

var     fromblock   =   0
process.argv.forEach( (val,index) =>
    {
        if ( ! isNaN(val) )
            fromblock   =   val<0 ?  web3.toHex(eth.blockNumber-2000) : val;
    }
);

function pastevent( ev )
{
    web3.eth.getBlock( ev.blockNumber, false )
    .then(
        (block) => {
            fromblock       =   ev.blockNumber + 1;
            var     d       =   new Date();
            d.setTime( block.timestamp * 1000 );
            var     t   =   "#" + ev.blockNumber + " <" + d.toUTCString() + ">: " + ev.event;
            Object.keys(ev.returnValues).forEach(
                (arg) => {
                    if ( isNaN(arg) )
                        t   +=  " " + arg + ": " + ev.returnValues[arg];
                }
            );
            console.log( t );
        },
        (x) => {
            console.log(x);
            process.exit(1);
        }
```

1,1 Top

Creating zone:
$ zone=robert.ar
$ serial=$(date +%s)
$ echo $serial other-stuff > zonas/$zone

Distributing
$ ipfs add zonas/$zone
added **QmbkgDbPRa2zdNq4F1V6VWNcm78XxY35K72jRcoeDEutPV** robert.ar
 33 B / ? [--=----------------------------------]
$ location=QmbkgDbPRa2zdNq4F1V6VWNcm78XxY35K72jRcoeDEutPV
$ symmetricpassphrase=pepe
$ enc_location=$(echo $location | openssl enc -e -a -aes-128-cbc -pass pass:$symmetricpassphrase)
U2FsdGVkX1+m9J3j7AJM+95TlgEYTgwh0WlYBwsnWNI=

Announcing:
$ bfapubzone $contractaddress $zone $serial $enc_location

robert@robertsbfasandbox:~$ docker ps | grep -v unhealthy
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES
bd5142ebd3e5 5d777da01ec3 "/home/bfa/bfa/bin/s…" 8 days ago Up 8 days (healthy) 127.0.0.1:8545->8545/tcp, 8546/tcp, 30303/udp, 0.0.0.0:30303->30303/tcp rlegene/bfanode

Contract events trigger script.
– (rfc 1982) compares serial
|– fetches zone + loads zone if serial is newer