



A survey of the peer to peer based DNS system

Who am I?

- Data Analyst @ Dyn
- Keeper of dogs
- Lover of Internet
- Hater of Ne'er do wells



The Year of The Crypto Currency



I swear I'm not making this up



Patrick M. Byrne
@OverstockCEO



Following

#Bitcoin's first full day on @overstock.com was a huge success: 840 orders, \$130,000 in sales. Almost all new customers. #stunned

← Reply ↻ Retweet ★ Favorite ⋮ More



Proof of Work as Stored Value

- Computer scientist Hal Finney built on the proof-of-work idea
- The idea of making proofs-of-work reusable for some practical purpose had already been established in 1999.
- The value of a proof of work token is guaranteed by the value of the real-world resources required to 'mint' a proof of work token.

What are Crypto Currencies?

- Amount of currency / units are controlled by fixed rules (not a central bank)
- Currency / Units are made available at a controlled rate to avoid inflation
- The transformation or storage of computational work and power spent doing work in a reusable unit

What is Namecoin?

- Derived from the Bitcoin codebase
- Stored units of work are called Namecoin
- Namecoin can be spent adding to or modifying the namecoin block chain
 - Registering names & updating resource records

Where it all began

- Started with BitDNS by Appamato in 2010
 - Design goal a distributed DNS
 - provide a distributed authority-free name allocation and transfer service
- The idea was picked up by Aaron Swartz
- Swartz looked at the implementation of the block chain in BitCoin and drew a parallel to a name system

Hard to site as first mention by Appamato is only in IRC logs ...

Squaring Zooko's Triangle

- Describes traits of a desirable naming system
- Choose two
 - secure
 - decentralized
 - human readable



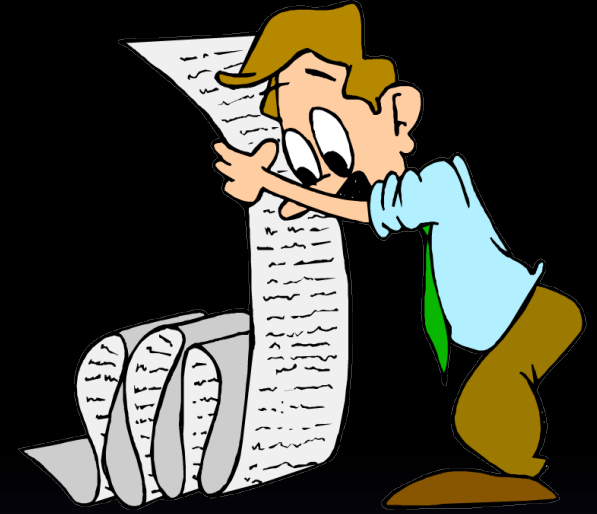
Nick Szabo has done some work which people agree has "Squared Zooko's Triangle"

Options

- Secure, Decentralized, Non-Human-Readable
 - eVsBkQCbxXahnqkmj8uekD4mV6y5Ve.dyn.com
- Secure, Centralized, Human-Readable
 - dyn.com verified by the DNS root (ICANN)
- Insecure, Decentralized, Human-Readable
 - dyn.com verified by peer consensus

Swartz's Summary:

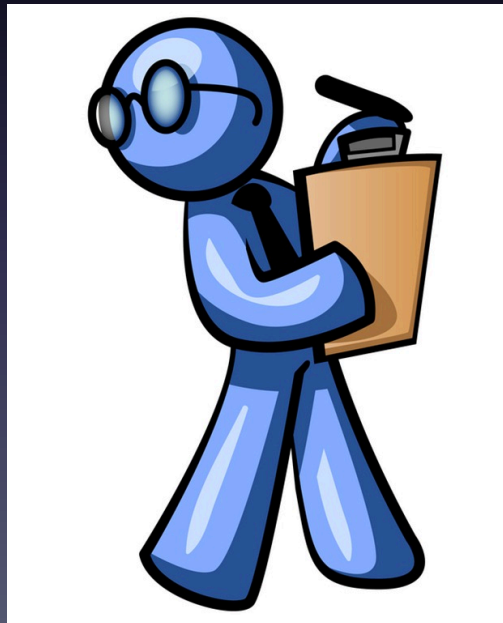
- There is a document called the scroll
- The scroll consists of a series of lines
- Each line consists of a tuple (name, key, nonce) such that the first N bits of the hash of the scroll from the beginning to the end of a line are all zero
- As a result, to add a line to the scroll, you need to do enough computation to discover an appropriate nonce that causes the bits of the hash to be zero.



- To look up a name, you ask everyone you know for the scroll, trust whichever scroll is the longest, and then start from the beginning and take the key for the first line with the name you're looking up.



- To publish a name, you find an appropriate nonce and then send the new line to everyone you know.



How could a name be stolen?

1. Calculate a new nonce for the line you want to steal and every subsequent line ...
 - Requires having some large multiple of the rest of the network's combined CPU power.
2. Get your replacement scroll to the user.
 - This seems a bit harder

Kaminsky Responds

- In the original draft existing names cannot alter their keys ... huge flaw #1
- Failure will occur in everyday use due to lack of transaction semantics

Kaminsky Responds

- Reconciling distributed transactions will cause chaos! Because it requires that additions happen sequentially.

Example

- We have a scroll with 131 name/key pairs
- Alice and Bob try to add a name without knowing about the other's attempt.
 - Alice will compute and distribute 131,Alice, and Bob will compute and distribute 131,Bob.
- What now? Which scroll should people believe? Alice's? Bob's? Both? Should they update both? How will this work over time?

Details, Details, Details ...

History Cont.

- December 09, 2013 - Special-Use Domain Names of Peer-to-Peer Systems
 - .bit is mentioned along side .onion, .gnu and others

Wide range of records implemented

- service - Used to identify hosts that support particular services as per DNS SRV records.
 - SRV "service": [["imap", "tcp", 0, 0, 143, "mail.host.com."]]
- ip - IPv4 addresses
 - A "ip": ["192.168.1.1", "192.168.7.1"]
- ip6 - IPv6 addresses.
 - AAAA "ip6": ["2001:4860:0:1001::68"]
- tor - Tor hidden service address.
 - "tor": "eqt5g4fuenphqinx.onion"

Wide range of records implemented

- l2p - Eepsite information. At least one hint is required.
 - "l2p": {
 "destination": "XaZscx...ojGAAAA"
 "name": "example.l2p"
 "b32" : "ukeu...nkdq.b32.l2p"
} freenet Freesite Key. - "freenet": "USK@oI8g...xbZ4,AQACAAE/Example/42/"
- alias - Specifies that this name is an alias of the given
 - Absolute domain names are signified by an added dot (.) CNAME
- translate - Specifies that all subdomains of this name are translated to the given String before lookup. As with alias, absolute domain names end with a dot (.)
 - Ex: "subdomain.test.bit" could be translated to "subdomain.otherhost.bit".
 - DNAME "translate": "otherhost.bit."
- ds - DNSSEC fingerprints for securing the domain when used with DNS via ns.
 - Format roughly mirrors RFC3658 - the fields are keytag, algorithm, hash type, and base64(hash(domain + DNSKEY RRDATA))
 - DS "ds": [[31381,8,1,"pA1W...ceTI="], [31381,8,2,"toHB...ndexitQ6j8E="]]

Reference : https://wiki.namecoin.info/index.php?title=Domain_Name_Specification_2.0

First Look – December 2013

How many names have been registered

What is the geographic distribution of IPs

What DNS record types are most common

What patterns have emerged in name registration

Old - Raw Record Counts (Dec 2014)

Count	Record type
14138	A
6115	NS
187	DNAME
51	CNAME
22	AAAA
2	DS

Old - Raw Record Counts

25521	Total DNS Records
527	Unique IPs
423	Unique Netblocks
264	Unique ASNs

Current State






How many names have been registered

What is the geographic distribution of IPs





What DNS record types are most common

What patterns have emerged in name registration

Raw Record Counts

Count	Record Type
 8494	A
 6600	NS
 29	CNAME
 29	DNAME
 27	AAAA
2	DS

Raw Record Counts

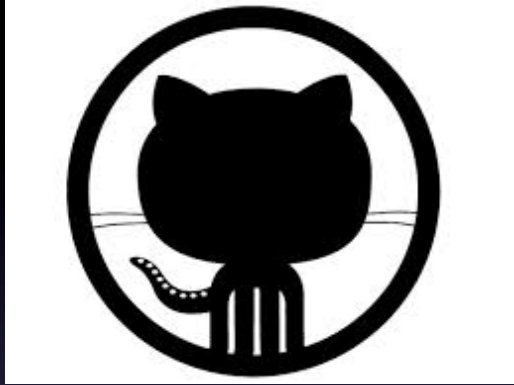
	15181	Total DNS Records
	610	Unique IP v4 Addresses
	472	Unique Netblocks
	287	Unique ASNs

The big take away here is registration of new domains continues, however squatters aren't creating resource records.

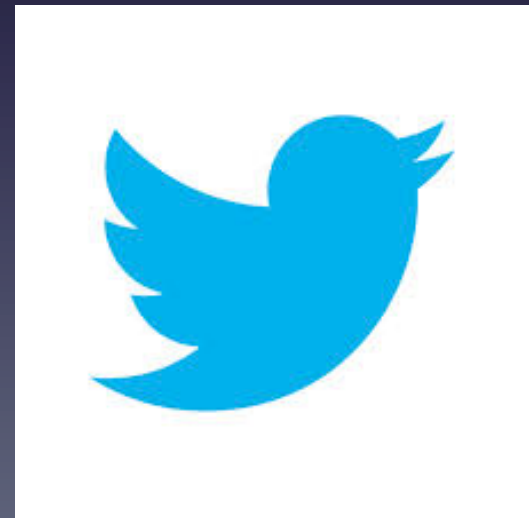
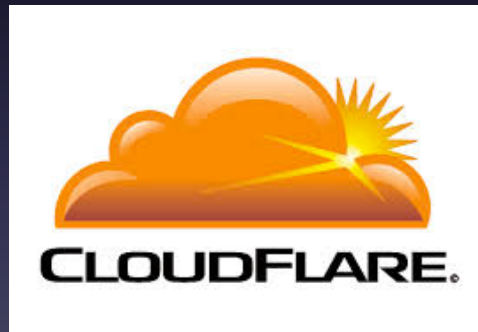
Count of IPs by Country	Country Code
328	US
42	DE
32	FR
32	GB
30	NL
21	CA
19	(NA) / Other
11	AU
8	SE

IP to ASN Mapping done using Team Cymru and ShadowServer

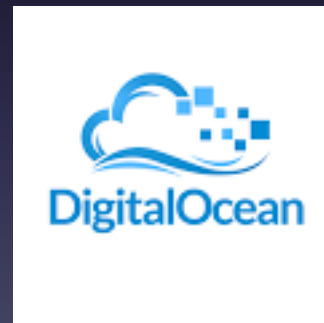
Surprise IPs



fastly[®]



Expected



Implementation Issues

- .bit isn't an ICANN approved TLD so custom configuration for resolution is required
- Accessing bit domains requires a copy of Namecoin blockchain or a supporting public DNS server or a proxy.

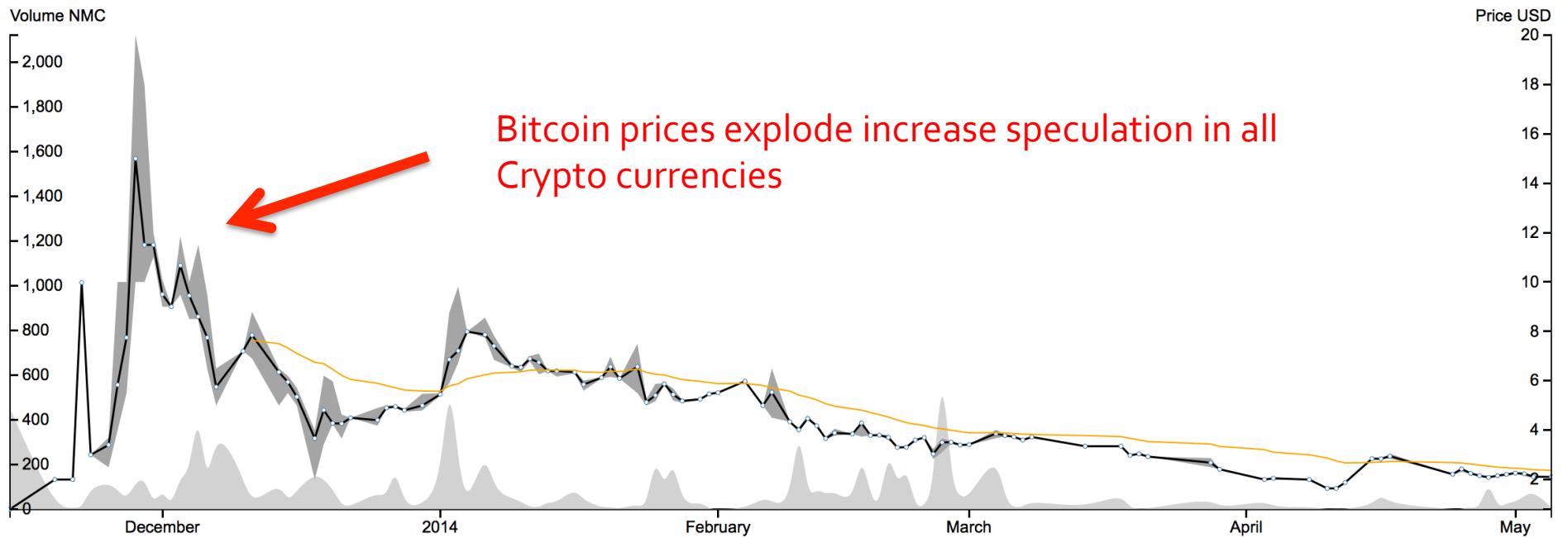
.Bit DNS Servers

<i>IP</i>	<i>Host</i>	<i>Country</i>	<i>Company</i>	<i>AS no.</i>
192.249.59.89	atl-dns-dotbit.synapse-axon.net	US, United States	RamNode LLC	AS3842
192.184.89.74	sea-dns-dotbit.synapse-axon.net	US, United States	RamNode LLC	AS3842
176.56.238.160	176.56.238.160	NL, Netherlands	RouteLabel V.O.F.	AS198203
95.211.195.245	lw177.ua-hosting.com.ua	NL, Netherlands	LeaseWeb B.V.	AS16265
64.31.48.60	60-48-31-64.static.reverse.lstn.net	US, United States	Limestone Networks, Inc.	AS46475
178.63.16.21	dotbit.me	DE, Germany	Hetzner Online AG	AS24940
178.32.31.41	dns.dot-bit.org	FR, France	OVH Systems	AS16276

Accessibility Issues

- Obtaining Namecoin is a whole different challenge
- To purchase Namecoin with USD you need to register with an exchange
 - To register with an exchange you need to give them PII (social security number, pass port photos ... etc)
 - So basically you need to buy bitcoin or trade

Historic – Price / Volume



Exchange Rate of NMC

Hourly Price History (NMC/USD)

Last Updated: 05-05-14 16:51:05 +00:00



Evil Side: Neccurs

- So you may ask, how do the bad guys leverage .bit domains if accessing them requires customization?
- Does it change proxy settings or it changes DNS settings of host? No it doesn't.

Neccurs Cont.

- Neccurs modifies the domain resolution path so if the TLD is .bit it changes the recursive
- It leverages the 'DnsQuery_W' parameter in the Windows API to specify the DNS server to send the query to

Challenges

- Domains cannot be taken down by traditional methods
- No one has the power to sinkhole the domain but its owner

The Blockchain is PassiveDNS!

- The blockchain contains the history of every record ever added or removed from .bit
- Tracking the IPs used by a malicious domain is simple

Lets looks at some interactions

Name : d/dnsoarc

Link : <http://explorer.namecoin.info/n/d/dnsoarc>

Date	Op	Block	Transaction	Value
17/04/14 01:32:18	OP_NAME_UPDATE	172309	1197021	{"ip":"149.20.58.8","map":{"*":{"ip":"149.20.58.8"}}}
27/03/14 21:23:27	OP_NAME_FIRSTUPDATE	168950	1143211	
27/03/14 20:01:15	OP_NAME_NEW	168936	1142946	Hash : 589a2813a6394159658c3cc3d46922686d95255c

Name : d/dns-oarc

Link : <http://explorer.namecoin.info/n/d/dns-oarc>

Date	Op	Block	Transaction	Value
17/04/14 01:32:18	OP_NAME_UPDATE	172309	1197012	{"ip":"149.20.58.8","map":{"*":{"ip":"149.20.58.8"}}}
26/03/14 03:42:01	OP_NAME_FIRSTUPDATE	168665	1136353	
26/03/14 02:04:20	OP_NAME_NEW	168650	1136193	Hash : 589b21ddc61a9c2787cf5d1fed9176e4be40949b

Popular Necurs .bit domain

Name : d/megashara

Link : <http://explorer.namecoin.info/n/d/megashara>

Date	Op	Block	Transaction	Value
16/10/13 08:31:41	OP_NAME_UPDATE	140099	850330	{"ip":"175.249.168.45"}
02/10/13 05:34:20	OP_NAME_UPDATE	137354	818297	{"ip":"234.106.33.60"}
18/09/13 05:37:14	OP_NAME_UPDATE	134581	800645	{"ip":"168.59.47.214"}
14/09/13 04:20:45	OP_NAME_UPDATE	133736	795627	{"ip":"37.129.224.126"}
10/09/13 15:10:38	OP_NAME_UPDATE	133212	789610	{"ip":"43.181.124.171"}
06/09/13 02:31:05	OP_NAME_UPDATE	132267	785860	{"ip":"168.187.206.194"}
31/08/13 18:16:35	OP_NAME_UPDATE	131244	783092	{"ip":"61.42.244.212"}
28/08/13 23:12:13	OP_NAME_UPDATE	130611	781483	{"ip":"172.136.7.39"}
26/08/13 09:37:31	OP_NAME_UPDATE	130064	779659	{"ip":"74.144.157.102"}
23/08/13 13:27:44	OP_NAME_UPDATE	129519	777679	{"ip":"32.202.157.199"}
20/08/13 09:53:31	OP_NAME_UPDATE	128948	776102	{"ip":"166.243.216.181"}
14/08/13 07:16:01	OP_NAME_UPDATE	127593	770659	{"ip":"35.138.136.205"}
10/08/13 00:53:38	OP_NAME_UPDATE	126691	767897	{"ip":"235.114.56.59"}
06/08/13 08:02:58	OP_NAME_UPDATE	125737	764972	{"ip":"61.42.244.212"}
02/08/13 10:13:39	OP_NAME_UPDATE	124925	762948	{"ip":"168.219.174.213"}
23/07/13 02:41:03	OP_NAME_UPDATE	123228	756131	{"ip":"58.125.199.202"}
17/07/13 22:34:44	OP_NAME_UPDATE	122354	753934	{"ip":"32.42.92.217"}
13/07/13 07:59:03	OP_NAME_UPDATE	121530	749385	{"ip":"167.187.171.199"}
10/07/13 06:27:50	OP_NAME_UPDATE	121022	743471	{"ip":"14.105.236.100"}
08/07/13 05:49:40	OP_NAME_UPDATE	120668	742520	{"ip":"17.107.180.139"}
04/07/13 14:29:53	OP_NAME_UPDATE	120028	740013	{"ip":"142.67.242.151"}

Bad Guys Respond

- As researchers started to track the malicious domains & the bad guys switched up tactics
- No longer did the .bit domain point to the IP of the C&C node but became a variable
- The IP returned from the query became the key that combined with the right transformations would yield the true C&C IP

Innovations!



DNSChain
=
Real ownership.



Your connection to the Namecoin blockchain.

DNSChain - DNSNMC

- Certificate Authorities make HTTPS and SSL /TLS insecure
- A protocol and browser extension that protects the content of almost all online text-based communication from a variety of threats (such as MITM)
- “trust only those you know” vs. “trust a bunch of untrustworthy strangers”

DNSChain - DNSNMC

- The Namecoin block chain acts as a distributed trusted data store
- Clients obtain DNSNMC server public key finger print and IP
- They use these details to verify their source of truth is what they think it is
- This is not perfect authentication ... "it provides authentication that is meaningful."