Intro to Namecoin

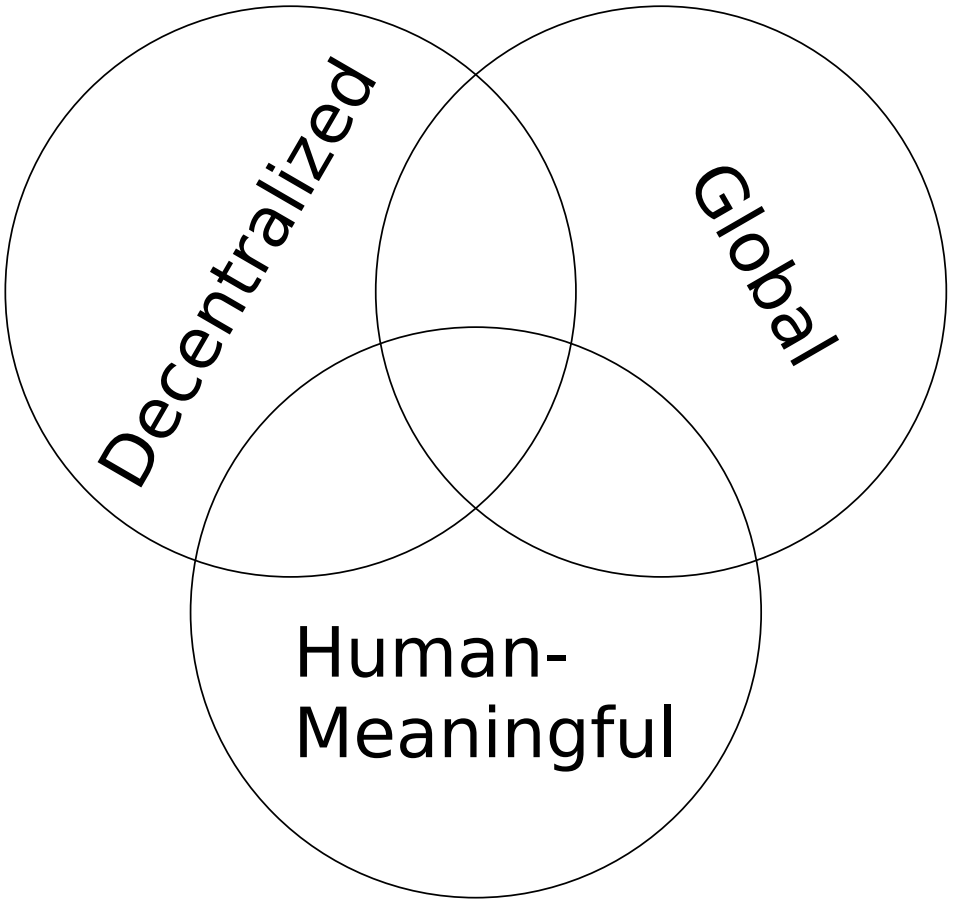
Jeremy Rand
Lead Application Engineer, The Namecoin Project
https://www.namecoin.org/

OpenPGP: 5174 0B7C 732D 572A 3140 4010 6605 55E1 F8F7 BF85

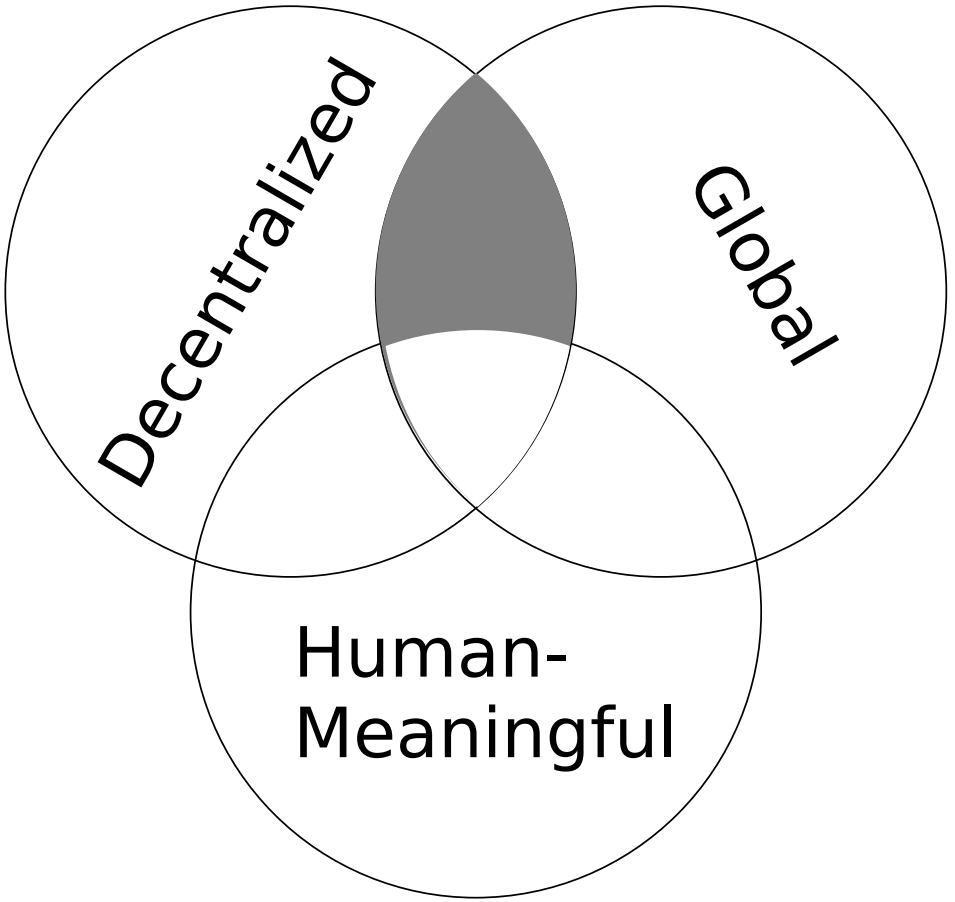
Presented at 36C3 Monero Assembly / Critical Decentralization Cluster

DNS

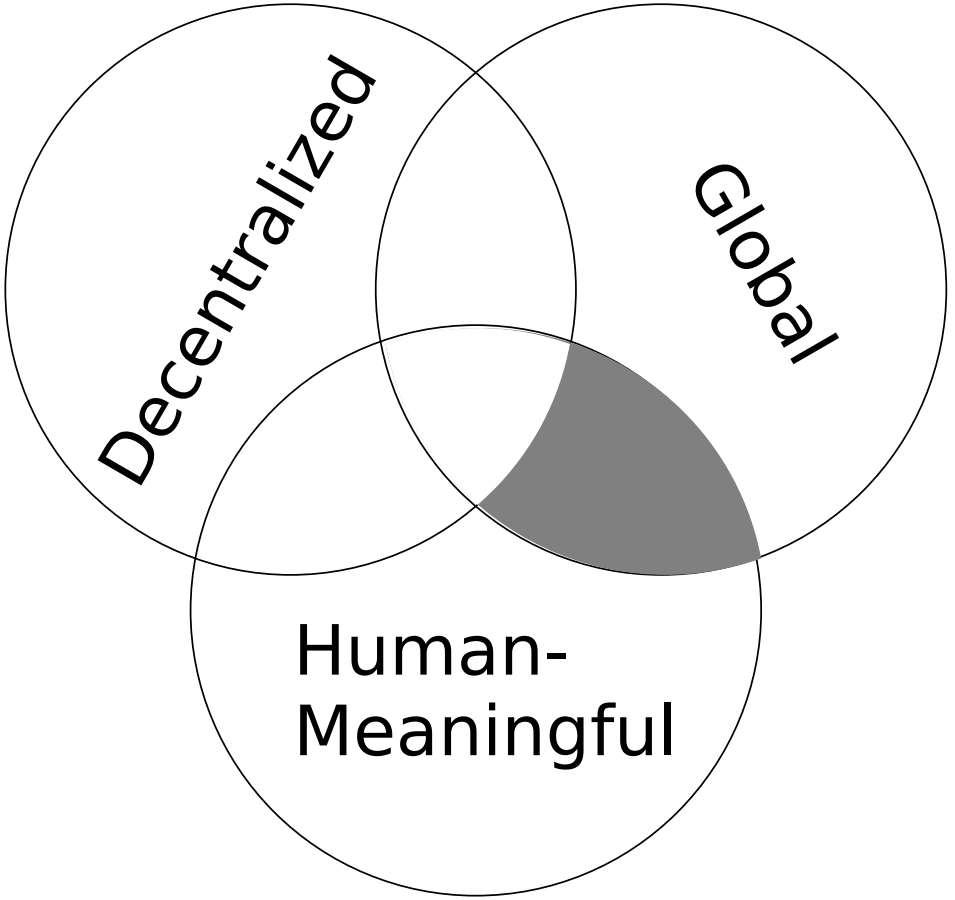
- DNS maps domain names to IP addresses.
- Vulnerable to censorship (making a domain name not resolve).
- Vulnerable to hijacking (making a domain name point to the wrong website).
- Because it’s too centralized.
- What features are “desirable” in a DNS-like system?



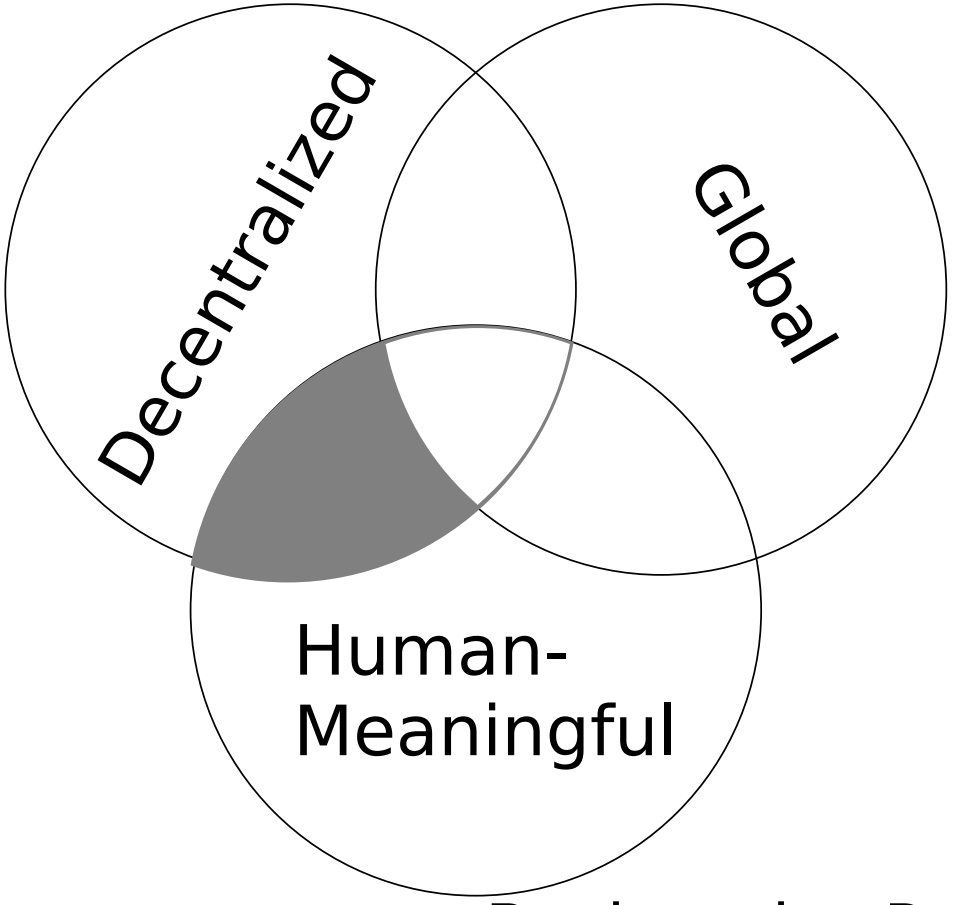
Zooko's Triangle: Choose any 2 of these 3



Not Meaningful: Crypto Keys, .onion domains



Not Decentralized: DNS, DNSSEC



Not Global: Bookmarks, Petnames, GNU Name System, I2P

Zooko’s Triangle is a **hard** problem

- Achieving all 3 properties of Zooko’s Triangle generalizes to the decentralized global consensus problem.
- First analyzed by Lamport in the 1970’s.
  - Lamport concluded that it was impossible.

Zooko’s Triangle is a **hard** problem

- Analyzed by Wikimedia when Wikipedia was being built.
  - They wanted to make Wikipedia a P2P app instead of running on central servers.
  - Ended up independently reproducing Lamport’s argument that it was impossible.
- Analyzed by the cypherpunk community in various efforts to build a P2P currency (the “double-spend problem”).
  - Concluded that it was impossible.

Bitcoin’s design is the solution

- The class of “decentralized global consensus” problems that includes Zooko’s Triangle was finally solved by Bitcoin in 2009.
- So can we solve Zooko’s Triangle with Bitcoin?

Appamatto’s Take

- Appamatto posted in the #bitcoin IRC channel in 2010.
- “I had an idea for a bitcoin-like DNS system. Basically, each generating block allows you to define a new name, and transactions are remappings of the names to ip addresses”
- “Although there have been attempts to tackle DNS in a distributed way in the past, I don't think there have been solutions that have fully removed authority from the equation.”

Appamatto’s Take (2)

- “If there was such a solution, it probably would have been able to implement bitcoin directly on top of it, and we all know that didn't happen.”
- Proposed BitDNS.

Theymos’s Take

- Theymos replied to Appamatto’s proposal.
- “Why not just generate ‘domain credits’ that allow you to generate a domain, and then transfer those around, too?”
- Allowed users to register names trustlessly without being a miner.
- Effectively invented the concept of the utility token.

Dan Kaminsky’s Take

- Dan Kaminsky and Aaron Swartz had been looking at Zooko’s Triangle for a while.
- Then Dan got interested in Bitcoin.
- Dan told Aaron that since DNS and a currency are similar problems, Zooko’s Triangle might make Bitcoin impossible too.

Aaron Swartz’s Take

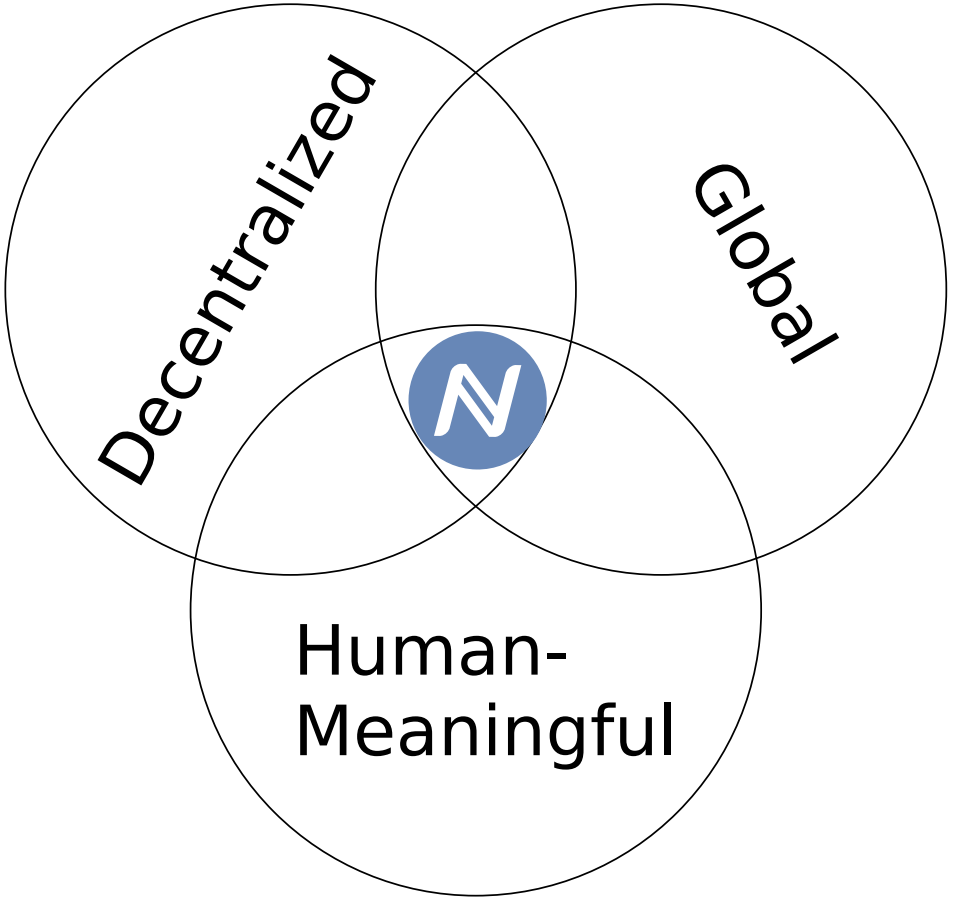
- Aaron pondered for a few days.
- And then concluded: Dan is actually right – but Bitcoin’s not impossible, it just means that we can use Bitcoin to solve Zooko’s Triangle.
- Proposed Nakanames.

A couple months later…

- Vincent Durham announced the release of Namecoin.

Namecoin: DNS, but on a blockchain

- Uses the .bit TLD.
- Censorship-resistant.
  - Censoring a .bit domain is roughly as difficult as freezing bitcoins.
- Hijacking-resistant.
  - Hijacking a .bit domain is roughly as difficult as stealing bitcoins.



Namecoin: Squares the triangle!

Namecoin as a decentralized public key infrastructure

- Need to look up a public key for TLS, Tor onion services, PGP, OTR/OMEMO, etc.? Namecoin can help.
- E.g. you can put a TLS certificate fingerprint in your .bit domain.
- And visitors to your website can verify your certificate without relying on a public CA.
- (Similar to what DNSSEC/DANE does, but without the ICANN root key.)

Cool Things About Namecoin

- Only non-Bitcoin cryptocurrency where Satoshi Nakamoto directly had a hand in development.
- Endorsed by WikiLeaks in 2011 (and mentioned by Julian Assange in his conversation with Google CEO Eric Schmidt).
- Favorably mentioned in a 2014 ICANN “Identifier Technology Innovation” report.

Cool Things About Namecoin (2)

- Favorably mentioned by Internet Archive founder Brewster Kahle in 2016.
- Utilized by the NSA whistleblowers “The Shadow Brokers” to leak NSA malware code without censorship in 2016-2017.
- New York Times alleged in 2018 that Saudi Arabian intelligence recruited a Twitter employee to spy on one of the Namecoin devs' Twitter accounts.

Namecoin loves collaboration

- E.g. we’re collaborating with Monero on enabling anonymous name registrations.
- If you have a cool idea for working with us, talk to me!
- The Namecoin logo on my shirt should help you find me.