Namecoin: Decentralized DNS-Like Identifiers

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

jeremy@namecoin.org
OpenPGP: 5174 0B7C 732D 572A 3140 4010 6605 55E1 F8F7 BF85

Slides co-written with Hugo Landau; Presented at ICANN58

Underlying motivation of Namecoin

- Humans and the systems they directly operate behave nondeterministically.
- This includes the DNS.
  - Will the policies you agreed to still be in place in 10-20 years?
  - DNS might be subject to political issues that you can't predict right now.

- If DNS weren't run by humans, it would be much easier to make reliable predictions about its future behavior.

- (H/t to Greg Maxwell's philosophical writings on this topic.)

Underlying motivation of Namecoin (2)

- Namecoin is an experiment to find out:
- Can we make something similar to DNS, but with minimal human involvement?
  - This could behave more deterministically than the DNS.
  - And be more reliable and secure against human-based failure modes.

Existing Identifier Systems: Manual naming at a site

- E.g. hosts file

No global namespace; names only meaningful locally

Safe from nondeterministic human third parties

Human-meaningful names

Existing Identifier Systems: Hierarchical naming

- E.g. DNS


Global namespace


Not safe from nondeterministic human third parties


Human-meaningful names

- Good usability.
- Risky as root of trust.

Existing Identifier Systems: The name is the public key

- E.g. Tor's .onion services

✓ Global namespace
✓ Safe from nondeterministic human third parties
✗ No human-meaningful names

- Safe as root of trust
- Poor usability: user sees ~~https://duxenkne4qt76ig.onion~~
  https://odmmeotgcfx65l5hn6ejkaruvai222vs7o7tmtllszqk5xbysola.onion

Zooko's Triangle

- You may have noticed in the preceding slides …
  - 2x ✓
  - 1x ✗
- This is Zooko's Triangle.
  - Zooko Wilcox conjectured that it was impossible to achieve all 3 of:
    - Global namespace
    - Safe from nondeterministic human third parties
    - Human-meaningful names

Namecoin

- Namecoin is a blockchain for name registrations and updates.
  - ✓ Global namespace
  - ✓ Safe from nondeterministic human third parties
  - ✓ Human-meaningful names

- Solves Zooko's Triangle.

TLS Public Key Infrastructure

- The Certificate Authority system is problematic (even with Certificate Transparency).
  - Way too many nondeterministic humans involved who can make mistakes.
- DNSSEC/DANE could improve the situation.
  - But the DNS root and the TLD operators are nondeterministic humans too – still not ideal.
- Namecoin could provide the advantages of DNSSEC/DANE without relying on nondeterministic humans.

Namecoin and DNS

- Namecoin has a DNS compatibility layer to translate DNS requests into Namecoin requests.
  - Makes installation relatively simple – just install Namecoin and the compatibility layer on your machine, and your applications that speak the DNS protocol will work with Namecoin.
- Namecoin uses the .bit TLD.
  - This is not registered with ICANN or IETF right now.
  - We'd like to find a workable way to register it, e.g. as a Special-Use Name (like .onion).

Namecoin Use Case: Buying and Selling Names

- In DNS, buying or selling a name usually involves some counterparty risk or relying on an escrow agent.
- In Namecoin, the buyer and seller can jointly construct a transaction that atomically pays the seller and transfers the name to the buyer.
- This eliminates counterparty risk without requiring an escrow agent's services.

- (Implementation by Phelix.)

Namecoin Use Case: Two-Factor Authentication

- Two-factor authentication can be implemented without fully trusting the 2FA service. Example policy:

- You can make arbitrary name updates with 2FA verification.
- You can revoke your TLSA record even if the 2FA service is down.
- If the 2FA service vanishes, you can recover your name after a given time period.
- The 2FA service can't issue any updates without your consent.
- Cryptographically verified; policies specified in a flexible scripting language.

- (Design based on GreenAddress in Bitcoin.)

Tradeoffs: Malware

- If a name is transferred to a new owner, the old owner can't get it back without the new owner's signature.
- This means that Namecoin names are somewhat more vulnerable to hostile takeover by malware.

- Workaround: store private keys on airgapped machines, or use 2FA!

Tradeoffs: Trademark Infringement

- Deterministic systems like Namecoin don't have a way to detect trademark infringement.
- Names can't be seized over trademarks.

- Workaround: users could opt into blacklists like PhishTank to detect fraudulent websites.

Tradeoffs: Privacy

- Namecoin transactions are public.
- Anyone can see whether multiple names have common ownership.
- Person who sold you your namecoin tokens knows what names you registered with them.

- Workaround: We're collaborating with blockchain privacy projects like Monero to give better privacy in the future.

Tradeoffs: 51% Attack

- Namecoin is based on “1 CPU, 1 vote”.
- If an attacker holds a majority of the computing power on the Namecoin network for an extended period of time, they could steal names.
- Very expensive attack to pull off, but much cheaper than directly attacking the elliptic curve cryptography.

- Workaround: the attack is easily detectable in real-time, so users could blacklist the hijacked name.
- We're also investigating ways to raise the cost of such an attack.

Direction of Development

- For average people, installing and using Namecoin is still relatively difficult.
- Especially if TLS is desired. (Which it should be.)
- We just received funding from the NLnet Foundation and the Internet Hardening Fund (with budget from the Netherlands Ministry of Economic Affairs); this funding will be used to improve usability and application support for Namecoin's usage as a TLS PKI.
  - This work is being done by Jeremy Rand, Hugo Landau, Brandon Roberts, and Joseph Bisch.

Thanks for inviting me!

- Happy to take questions.

- https://www.namecoin.org/
- My email: jeremy@namecoin.org
- My OpenPGP:
  5174 0B7C 732D 572A 3140 4010 6605 55E1 F8F7 BF85