namecoin

Namecoin: NGI Projects

Lola Rigaut-Luczak (principal investigator)
Yanmaani (principal investigator)
Ahmed Bodiwala (developer)
Jeremy Rand (presenting)

The Namecoin Project
https://www.namecoin.org/

Presented at the European Commission, December 2020

What is Namecoin?

- Namecoin is a naming system.
  - You can register domains like europa.bit.
- Has a global namespace (like the DNS).
- Names are human-meaningful (like the DNS).
- But… it is also decentralized.
  - No trusted third parties who can hijack or tamper with a name.

Under the hood

- Namecoin is a fork of Bitcoin.
  - Actually the first project forked from Bitcoin (2011).
- Names in Namecoin look like coins in Bitcoin.
  - Stealing/hijacking someone’s name without their private key is about as hard as stealing bitcoins.
- Uses the “.bit” TLD.
  - Requires Namecoin software to resolve (similar to “.onion” TLD requiring Tor software).

Use case: Namecoin as a replacement for public TLS certificate authorities

- The TLS ecosystem (used by HTTPS) currently relies on public certificate authorities (CA’s).
  - A compromised CA can enable impersonation of websites / traffic interception (“man in the middle” / MITM).
- Namecoin can embed a TLS public key directly in a domain record.
  - Removes the need to trust public CA’s.
  - Similar to DANE in the DNS world (embedding TLS public keys in a DNS record), but decentralized.

Namecoin TLS interoperability

- Mainstream TLS implementations don’t know how to validate certificates using Namecoin.
  - They mostly don’t even know how to use DANE.
  - Lack of browser support is a major reason almost no one uses DANE.
- Most other custom TLS certificate validation projects just use an intercepting proxy for interoperability.
  - We don’t do this – we think there’s too much attack surface there.

Namecoin TLS interoperability (2)

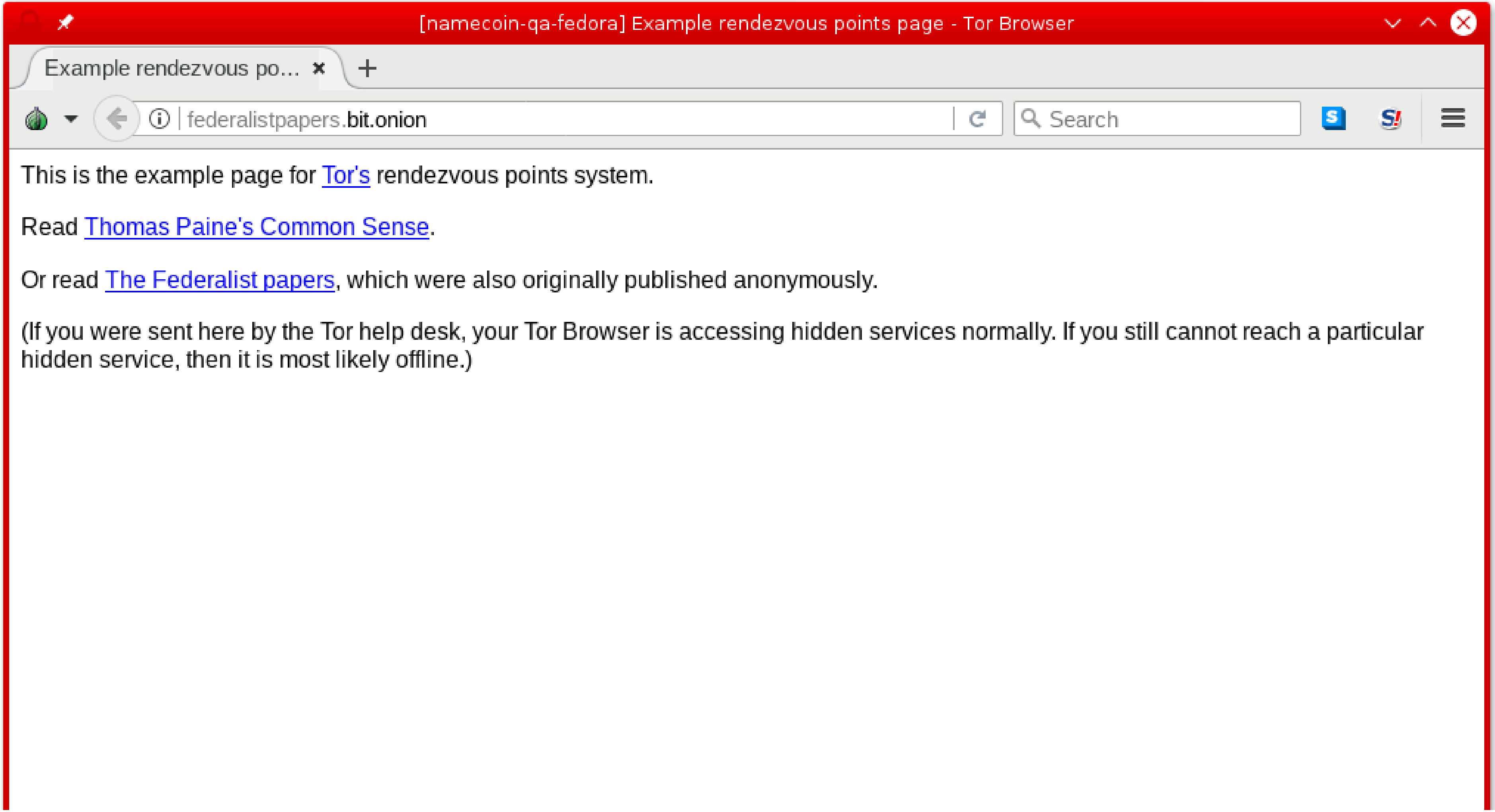
- We are innovators in customizing TLS certificate validation (of mainstream, unpatched browsers) with minimal attack surface.
- We use a variety of TLS API’s and features to achieve this, including:
  - PKCS#11
  - Dehydrated certificates
  - Imposed name constraints
  - Cross-signed name constraints
  - Windows registry blobs
  - AIA
  - Key pinning

Use case: Namecoin as a naming layer for Tor onion services

- Tor’s onion services feature (the “.onion” TLD) allows anonymous hosting of TCP services (e.g. websites).
  - Great for privacy, but the names are impossible to remember.
  - http://7fa6xlti5joarlmkuhjaifa47ukgcwz6tfndgax45ocyn4rixm632jid.onion/
  - Users will often not check the entire name.
  - Enables phishing attacks.
- Namecoin domains can point to a Tor onion service instead of an IP address.
  - Acts as a human-meaningful naming layer for onion services.
  - E.g. http://federalistpapers.bit/ is an alias for the above onion.

Namecoin Tor interoperability

- We integrated Namecoin into Tor.
- Preserves Tor’s anonymity/security properties for name lookups.
- Good performance due to optimized lightweight Namecoin client.
  - Ready to resolve names within a few seconds of starting Tor Browser.
  - Works with a normal, unmodified Tor Browser.
  - Testers report speed indistinguishable from regular “.onion” websites.



[namecoin-qa-fedora] Example rendezvous points page - Tor Browser
Example rendezvous po…
federalistpapers.bit.onion
Search

This is the example page for Tor's rendezvous points system.

Read Thomas Paine's Common Sense.

Or read The Federalist papers, which were also originally published anonymously.

(If you were sent here by the Tor help desk, your Tor Browser is accessing hidden services normally. If you still cannot reach a particular hidden service, then it is most likely offline.)

What is ZeroNet?

- Use case looks a lot like HTTP.
  - ZeroNet is usually used for browsing websites, not file sharing.
- Implementation looks a lot more like BitTorrent.
  - No servers; website is served by other visitors.
  - Can be more reliable than HTTP (server outages aren’t a thing).
  - Can be more secure than HTTP (website content is signed).
    - ZeroNet addresses are public key hashes.

What is ZeroNet? (2)

- Supports Tor onion services as a transport.
  - Better privacy than BitTorrent.
- Supports Namecoin as a naming layer.
  - Human-meaningful names.
  - Unfortunately uses a centralized Namecoin resolver by default.
    - We’re going to fix this.

Adoption Trends

- Earliest adopter: ZeroNet. Couldn’t use existing systems like the DNS, didn’t have a huge pre-existing user base, experimentation was cheap and potentially high-reward.
- Subsequent adopter: Tor. Larger project who still is averse to the DNS, but has a large user base and needs to tread carefully to protect that user base.
- Later adopter: TLS. Might benefit from Namecoin, but could maybe get by with the DNS too, and needs to fight a lot of inertia.

Adoption Takeaway

- It’s not necessary (nor feasible) for everyone to adopt something like Namecoin all at once.
- Niche use cases can be a valuable foothold to wider adoption later.

Namecoin’s NGI Project Objectives

- Overhaul default ZeroNet usage of Namecoin.
  - Security and UX enhancements.
- Package Namecoin for GNU/Linux distros.
  - Is a prerequisite given by distros who have expressed interest in bundling Namecoin support by default.
- Add security, performance, and UX enhancements to core blockchain code.

Thanks for inviting us!

- And thank you for supporting Namecoin development!
- https://www.namecoin.org/
- OpenPGP (copy down our fingerprints!):
  - Lola:
    A10C F7F7 4B7B A003 98D4 9E3C 01E8 48E2 DDB4 874E
  - Yanmaani:
    C655 39F6 D216 23B3 CD95 5C81 95F1 4A60 0941 258C
  - Jeremy:
    5174 0B7C 732D 572A 3140 4010 6605 55E1 F8F7 BF85