A Blueprint for Making Namecoin Anonymous

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 34C3 Monero Assembly / Chaos West Stage

A brief introduction to Namecoin

- Like the DNS, but secured by a blockchain.
- Uses the “.bit” top-level domain.
- Names are represented by special coins.
- First project forked from Bitcoin (in 2011; Bitcoin was created in 2009).
- Original focus of developers was on censorship-resistance.
  - We later became interested in privacy use cases as well.

This talk is different from my previous 2 talks here

- My talks yesterday and earlier today were about things that are implemented and released.
- This talk is about an unimplemented rough plan.
  - Please help poke holes in the plan.
  - It's already been reviewed by a lot of people...
  - But more eyes on the design before implementation would be incredibly helpful.

Namecoin isn't currently anonymous

- And we view that as a big problem.
- We've been contacted by multiple users in the past who want advice on using Namecoin anonymously.
  - At least one of those users implied that their career could be unjustly ended if they got deanonymized.
- We want to support this use case – anonymous speech is a fundamental human right.

The obvious solution

- We could softfork to add ring signatures, or zk-SNARKs, to the Namecoin validation rules.
- This is the standard way that a currency blockchain would implement anonymity.
- But we're not a currency blockchain – does this matter?

Problems with the softfork anonymity approach

- We would be competing with Monero and Zcash in the “anonymous currency” market.
  - We prefer to collaborate with other projects rather than compete with them.
- We would have to choose either Monero or Zcash on behalf of users.
  - Users should be able to make their own decisions about what anonymity tech they use.
  - What happens when a new anonymous currency comes along? What if it's debatably better than Monero and Zcash?

Problems with the softfork anonymity approach (2)

- Scalability issues
  - Ring signatures and zk-SNARKs can't be pruned, and scale more poorly than the ECDSA signatures that Namecoin uses.
- Anonymity set
  - At best, your anonymity set is restricted to the set of Namecoin users (because you're anonymized after you obtain some Namecoins).
  - This may not be sufficiently anonymous.

So what can we do?

- We can realize that anonymity in a naming system is inherently different from anonymity in a currency.
- An anonymous currency implies that no two transactions by the same person are linkable as such.
- This makes no sense in the context of a naming system.
  - Multiple transactions for the same name will inherently be linkable as such.
  - And that's not problematic in any way.

Defining anonymity for a naming system

- We can define an anonymous naming system as follows: your transactions for a given name cannot be linked to any activity you performed that didn't involve that name.
  - This means that your distinct names aren't linkable to each other.
  - It also means that your names aren't linkable to your currency transactions.

A revised approach to an anonymous Namecoin

- Alice has some Monero; she wants to register a name anonymously.
- Bob has some Namecoins; he wants some Monero.
- Alice and Bob exchange Monero for Namecoin.
- Alice can now register a name. Bob (or a blockchain surveillance company) only can trace Alice's identity as far back as the Monero transaction, at which point the trail goes cold.

Benefits

- Namecoin doesn't compete with Monero or Zcash.
- Users can individually choose Monero, Zcash, or any other anonymous cryptocurrency.

Benefits (2)

- Users who only want to read name data don't need to download any Monero or Zcash transactions – only the Namecoin blockchain
  - Much more scalable.
  - 100% of Internet users read from the DNS; a much smaller fraction write data to the DNS.
- Anonymity set is the full Monero or Zcash anonymity set.
  - Because anonymization is done before purchasing Namecoins.

Bisq is incredibly well-suited for this

- Bisq already has a decentralized, private, censorship-resistant cryptocurrency exchange.
  - I've done some security/anonymity review for the Bisq devs – they're clearly competent and strongly care about these topics.
- It seems entirely feasible to utilize Bisq (perhaps with a custom UI) to create a user-friendly workflow for buying a Namecoin name with Monero.

Atomic Cross-Chain Trades

- This workflow could be made more trustless by using atomic cross-chain trades.
  - Easier for Zcash than Monero, since Zcash is more similar to Bitcoin.
  - Still totally feasible for Monero though.

Coin selection

- Once Namecoins are obtained anonymously, the wallet shouldn't mix coins from different names.
- This is a fairly straightforward rule to add to a wallet application.
- If all your coins are tainted by known name ownership, you'll need to buy more Namecoins with Monero.
  - And maybe sell your tainted Namecoins for Monero.
  - Is this an undue burden that will annoy users? I'm not certain – what do you think?

Open question: transaction amounts

- Does the amount of NMC that a user purchases form sufficient metadata to deanonymize users?
- We could standardize the amount that gets purchased.
- I'm curious what you think about this.

Open Invitation: Let's Collaborate!

- I'd love to see an active collaboration between Namecoin, Monero, and Bisq on this topic.
- Let's bring anonymous decentralized naming to the mainstream!

Contact Me At...

- https://www.namecoin.org/
- OpenPGP:
  5174 0B7C 732D 572A 3140 4010 6605 55E1 F8F7 BF85
- jeremy@namecoin.org
- Or just find me here at the Congress! (The Namecoin logo on my shirt should help you find me.)