Neutrino: Peer-to-peer private cryptographic currency with integrated Tor hidden services

Adam King
adam@neutrinocoin.org

John Reitano
john@neutrinocoin.org

1 March 2014
Revised: 9 June 2014

Abstract. Neutrino is a private cryptographic currency based on Litecoin, a variation of Bitcoin that replaces the SHA256 hashing algorithm with Scrypt for proof-of-work. Tor, an open-source software for enabling online anonymity and resisting censorship, is directly integrated into the core protocol as a hidden service, enabling nodes in the network to communicate anonymously. The resulting distributed network is highly resistant to third party eavesdropping and censorship. Neutrino is implementing Mixcoin in 2014 to ensure transactional privacy on top of the identity privacy provided by Tor.

1. Introduction

Recent revelations about government eavesdropping underscore the growing need for digital privacy, especially as society becomes increasingly reliant on information technology and the Internet. One of the most important applications of information technology is financial transaction systems. While Bitcoin revolutionized the way money is exchanged, it is not inherently private. In fact, with Bitcoin, both your digital identity and transaction history are given away by default.

Neutrino is a digital cryptographic currency designed to make financial transactions private by default in much the same way that secure connections (SSL) are now the default choice for most Internet communication and commerce. Neutrino directly integrates Tor into its core protocol, making each Neutrino node a Tor hidden service on the network. This enables a distributed, anonymous and end-to-end encrypted network that is highly resistant to third party eavesdropping and censorship.

Neutrino is based on Litecoin, a variation of Bitcoin that replaces the SHA256 hashing algorithm with Scrypt for proof-of-work.

2. Tor

Tor is a network of virtual tunnels that allows people to protect their privacy and security on the Internet by enabling them to share information over public networks without revealing their identity.

Tor was originally designed and implemented by the U.S. Naval Research Laboratory in order to protect government communications. Since its inception, it is now used every day by a wide variety of people including the military, journalists, law enforcement officers and activists. This variety is part of what makes Tor secure. The larger and more diverse Tor's user base is, the more your anonymity will be protected.

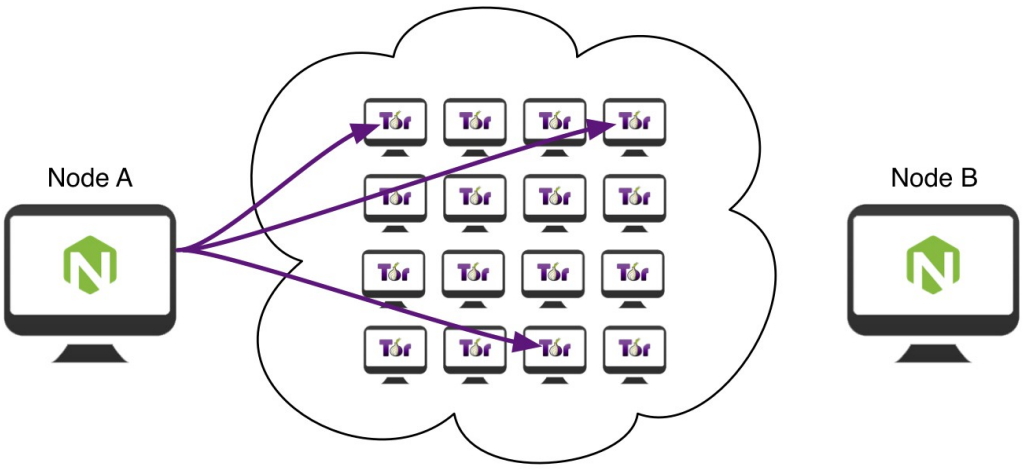
For more information on how Tor works, visit
https://www.torproject.org/about/overview.html.en

3. Hidden Services

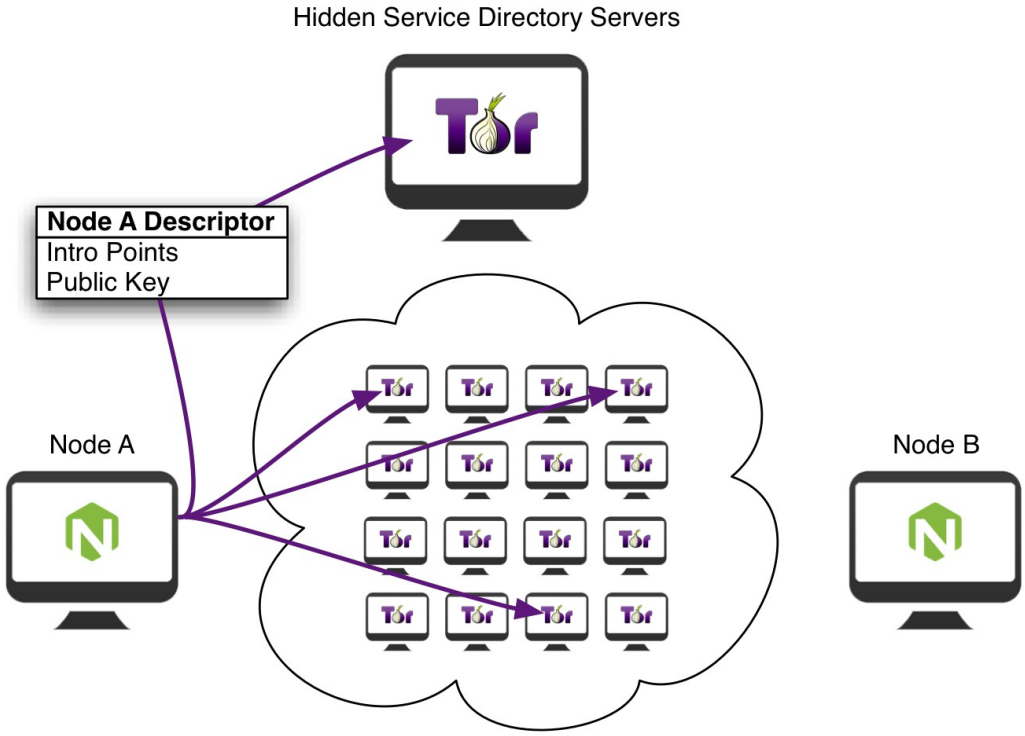
Neutrino uses a specific feature of Tor called hidden services to connect nodes in the network. Neutrino nodes connect to each other via rendezvous points without ever knowing each other's location. This enables users to use Neutrino without worrying about revealing their identity or being subject to censorship.

4. Communication Between Nodes

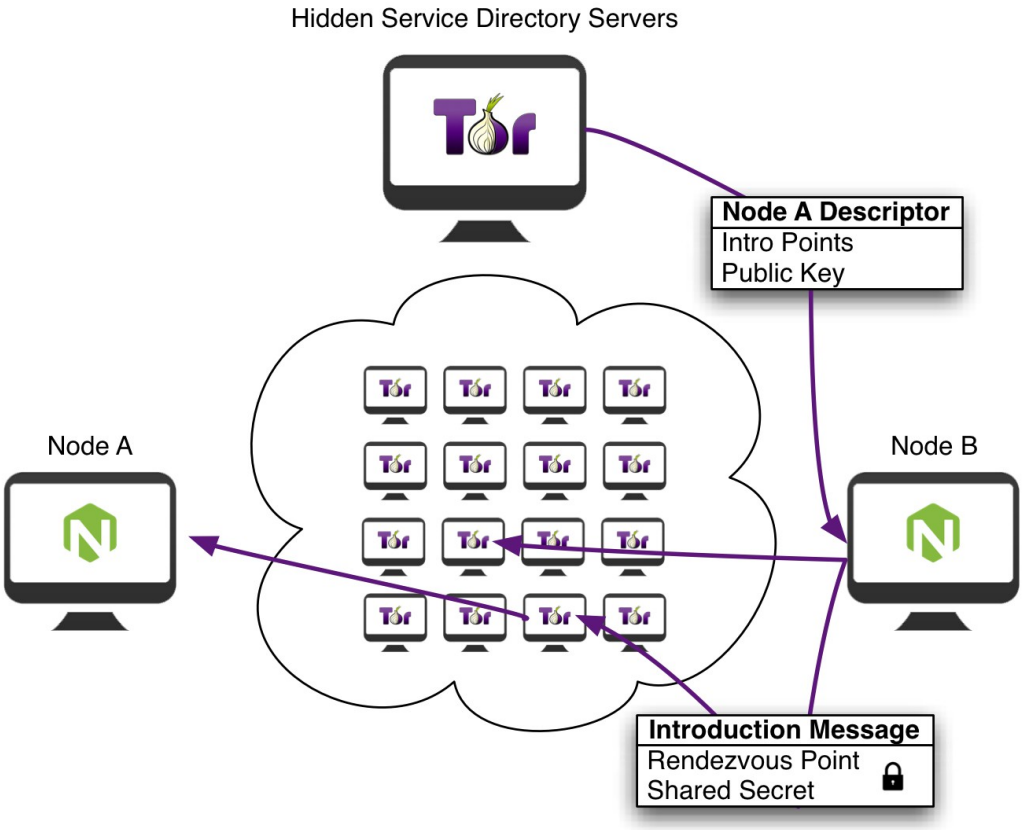
4.1. Each node in the Neutrino network creates its own hidden service. In order for nodes to be able to contact each other, each node must first broadcast the existence of its hidden service. To do so, the node automatically and randomly selects several Tor relays builds a full Tor circuit to them. By sharing its public key with the relays, the relays are able act as introduction points to other Neutrino nodes. The introduction points are only told the hidden service's public key and not the hidden service's location.



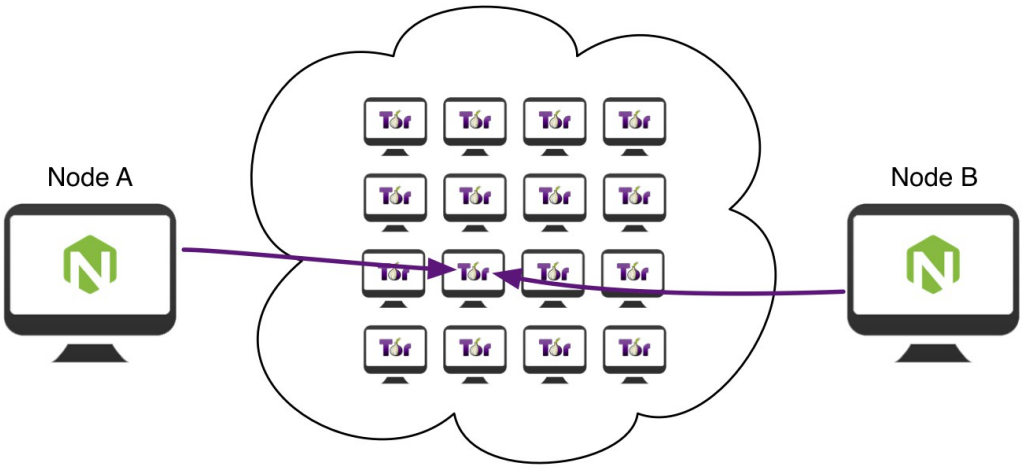
4.2. The node then packages a hidden service descriptor which contains the hidden service's public key along with a list of each previously selected introduction point. It signs this descriptor with its private key and uploads the signed descriptor to distributed Tor nodes known as Hidden Service Directory Servers. Other Neutrino nodes can then fetch the descriptor and use it to locate and connect to the hidden service via its onion address, a 16-character name derived from the hidden service's public key.



4.3. In order for one node to connect to another, it must first know the onion address of the target node's hidden service. An initial list of onion addresses is downloaded from a list of hardcoded seed nodes and maintained in a distributed fashion in much the same way that Bitcoin stores peer data. A node initiates a connection by downloading the hidden service descriptor from Hidden Service Directory Servers and selecting a random Tor relay as a rendezvous point for the connection. The node packages an introduction message with the address of the selected rendezvous point and shared secret and encrypts the package with the hidden service's public key originally obtained from the hidden service descriptor. The package is then delivered to the hidden service through one of the introduction points.



4.4. The rendezvous point then notifies the requesting node when it successfully connects to another node's hidden service. The requesting node and the target node's hidden service can now use their Tor circuits to the rendezvous point to communicate with each other.



5. Tor Relays

The Tor network heavily relies on relays to maintain the strength, speed and stability of the network. Each Neutrino node already has the ability to act as a Tor relay. While this feature is presently turned off by default, future versions will have this feature turned on by default.

The relationship between Tor and Neutrino is highly symbiotic: the more Neutrino nodes there are, the more Tor relays there will be and the more Tor relays there are, the faster and more reliable the Neutrino network will be.

6. Identity Privacy

By ensuring that all nodes in Neutrino's network communicate solely using Tor hidden services, users can operate the Neutrino client knowing that their location will not be revealed. This greatly protects the stability and security of the network while maintaing the user's privacy.

7. Resistance to Censorship

Neutrino's network is also highly resistant to censorship by oppressive governments. Due to the privacy of the identity of each Neutrino node coupled with end-to-end encrypted communication, the network can exist globally without bounds.

8. Transactional Privacy

While Tor integration allows for identity privacy and resistance to censorship, it only addresses part of Bitcoin's privacy problem and thus is an incomplete solution. Perhaps the Bitcoin protocol's most serious privacy vuerability is the manner in which transactions are linked in the blockchain. You can read more about this in:

> *A Fistful of Bitcoins: Characterizing Payments Among Men with No Names*
> http://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf
>
> *Bitcoin Transaction Graph Analysis*
> http://people.csail.mit.edu/spillai/data/papers/bitcoin-transaction-graph-analysis.pdf
>
> *Quantitative Analysis of the Full Bitcoin Transaction Graph*
> https://eprint.iacr.org/2012/584.pdf

Neutrino will be implementing its own version of Mixcoin, a protocol described in *Mixcoin: Anonymity for Bitcoin with accountable mixes* (http://eprint.iacr.org/2014/077.pdf). The implementation will be a joint effort between Neutrino core developers and university based cryptographic experts and will be integrated into Neutrino's core protocol in 2014.

For more information visit neutrinocoin.org

Protecting your privacy doesn't stop with Neutrino. We highly encourage you to support the following causes:

The Tor Project
https://www.torproject.org/

The Electronic Frontier Foundation
https://www.eff.org/

The Internet Defense League
http://www.internetdefenseleague.org/

The Free Software Foundation
http://www.fsf.org