Initial Discussion Paper for the TRI System

Matthew L. Hooft

The Amity Network

Author Note

Privacy is a right, not a privilege…

I would like to acknowledge my mom because she always told me I was cool.

Get at me via email at amitynetwork@protonmail.com or on discord at http://chat.amity.network

Abstract

The Tor Relay Incentive (TRI) System if implemented will be a system where Tor relay and exit operators will be able to register their nodes and receive rewards on the Amity Network. I am a firm believer in the right to privacy and support the Tor project as they help millions around the world daily avoid censorship and protect their privacy. Rewarding volunteers that participate in helping make the Tor network what it is will be a worthwhile endeavor and hopefully bring the Amity Network strong new allies.

Keywords: Anonymity, tor, privacy, TRI, Amity, wen, moon, derp, mitties

The TRI System and the Amity Network

Alpha Basic implementation

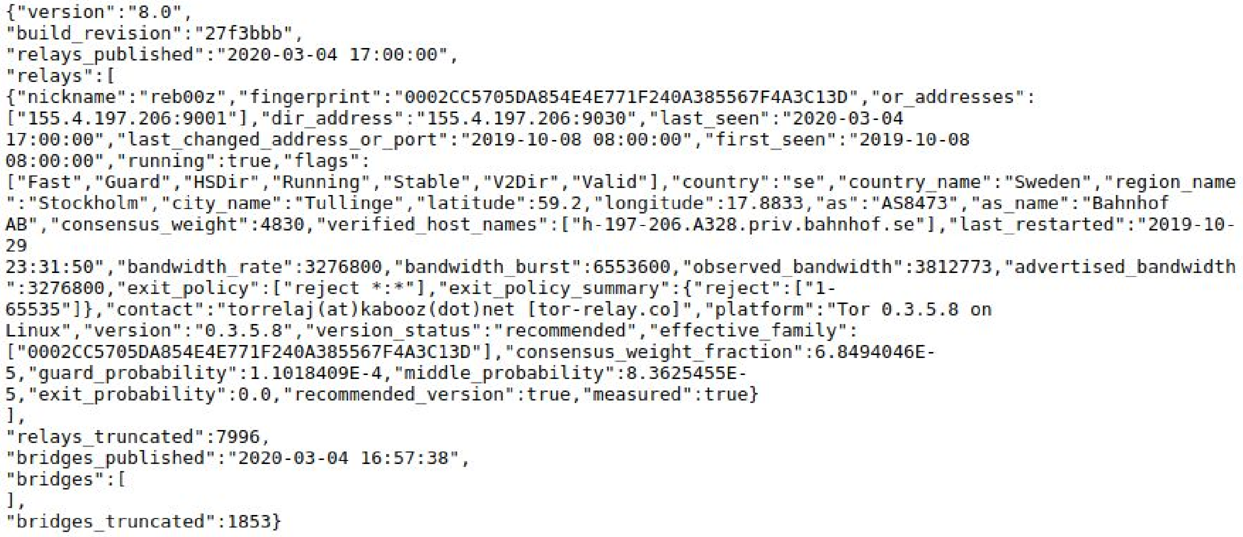
The Alpha implementation of the TRI system will, unfortunately, be a centralized one. To allow for decentralized rewards would require massive overhauls to the existing codebase that we are not prepared to make. This could possibly harm privacy which is paramount above else so it is felt that a centralized TRI protocol is acceptable as long as the network itself remains decentralized. Explained in the following is how we will attempt to implement the TRI Protocol Alpha.

Centralized Relay Registration Manager (RRM)

The Alpha implementation of the TRI System will utilize a centralized Relay Registration Manager or “RRM”. This will be a hosted Web Application that will handle registration and management of user accounts associated with tor relays and exits that want to receive rewards. While this service will be centralized, users will be allowed to remain anonymous while registering. This will be achieved by using Wallets Public addresses and Secret view keys to log in. This data will be handled in such a way that it is stored securely and encrypted while in transit. The RMM will require the Secret View Key as spam prevention stopping malicious actors from registering public addresses that they have somehow gotten ahold of to grief the system. It will also provide the RMM the ability to create view only wallets which will be used to verify rewards are being received at a registered address. View only wallets will only show **incoming** transactions so user privacy is still preserved to a reasonable degree.

The onionoo API

The RRM will utilize the onionoo API (https://metrics.torproject.org/onionoo.html) provided by the Tor project. This is an API designed to serve metrics and data about running relays, exits, and bridges that can be utilized by developers to create tools such as the RRM.



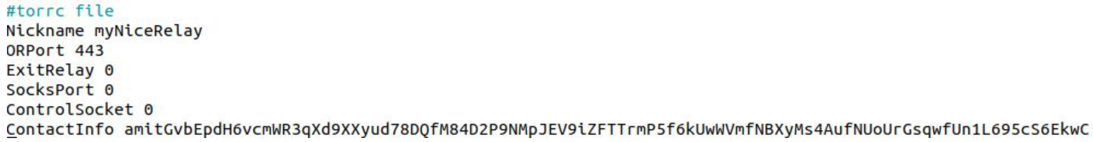
```
{"version":"8.0",
"build_revision":"27f3bbb",
"relays_published":"2020-03-04 17:00:00",
"relays":[
{"nickname":"reb00z","fingerprint":"0002CC5705DA854E4E771F240A385567F4A3C13D","or_addresses":
["155.4.197.206:9001"],"dir_address":"155.4.197.206:9030","last_seen":"2020-03-04
17:00:00","last_changed_address_or_port":"2019-10-08 08:00:00","first_seen":"2019-10-08
08:00:00","running":true,"flags":
["Fast","Guard","HSDir","Running","Stable","V2Dir","Valid"],"country":"se","country_name":"Sweden","region_name
":"Stockholm","city_name":"Tullinge","latitude":59.2,"longitude":17.8833,"as":"AS8473","as_name":"Bahnhof
AB","consensus_weight":4830,"verified_host_names":["h-197-206.A328.priv.bahnhof.se"],"last_restarted":"2019-10-
29
23:31:50","bandwidth_rate":3276800,"bandwidth_burst":6553600,"observed_bandwidth":3812773,"advertised_bandwidth
":3276800,"exit_policy":["reject *:*"],"exit_policy_summary":{"reject":["1-
65535"]},"contact":"torrelaj(at)kabooz(dot)net [tor-relay.co]","platform":"Tor 0.3.5.8 on
Linux","version":"0.3.5.8","version_status":"recommended","effective_family":
["0002CC5705DA854E4E771F240A385567F4A3C13D"],"consensus_weight_fraction":6.8494046E-
5,"guard_probability":1.1018409E-4,"middle_probability":8.3625455E-
5,"exit_probability":0.0,"recommended_version":true,"measured":true}
],
"relays_truncated":7996,
"bridges_published":"2020-03-04 16:57:38",
"bridges":[
],
"bridges_truncated":1853}
```

Example of Relay info returned in JSON

With the info provided by onionoo, the RRM will be able to poll the API for data ensuring registered relays and exits by the user are actually eligible for rewards.

Registration of Relays/Exits

After creating an account with the RRM using your address and secret view key, you will need to register your relay or exit. Before registering, you will need to add your public address to the contact info field in your ***torrc file.*** Once the public address is active on your relay you will submit your relays "fingerprint" to the RRM and it will be able to check the onionoo API for your relay and if the contact info matches your public address your relay will be registered and eligible for daily rewards.



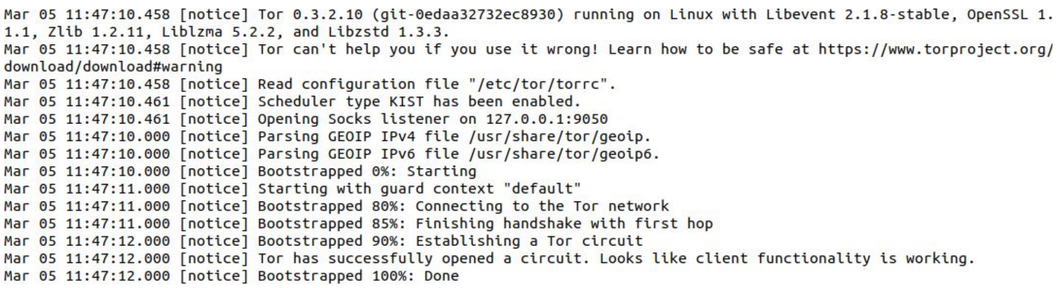
```
#torrc file
Nickname myNiceRelay
ORPort 443
ExitRelay 0
SocksPort 0
ControlSocket 0
ContactInfo amitGvbEpdH6vcmWR3qXd9XXyud78DQfM84D2P9NMpJEV9iZFTTrmP5f6kUwWVmfNBXyMs4AufNUoUrGsqwfUn1L695cS6EkwC
```

Example of a torrc file

Users will be able to register multiple relays or exits by submitting more fingerprints as long as the user's public address is being advertised as the relay's contact info. The more relays and exits a user operates, the more daily rewards a user will receive.

Relay Registration Manager Rewards System (RRMRS)

The RRM will have a secondary backend that will handle payments of rewards to participants in the TRI System. This will be handled using the Amity Wallet RPC and a centralized wallet. The RMM will maintain a database of active registered relays and exits and the RRMRS will use an algorithm that utilizes this data to determine how much daily rewards users will receive out of the daily pool available. This algorithm will use multiple factors to determine the number of rewards you receive. The factors will include but not be limited to, whether the node is a relay or exit, amount of uptime and bandwidth. The idea is the more resources you are able to contribute to the Tor network the more daily rewards you will receive.



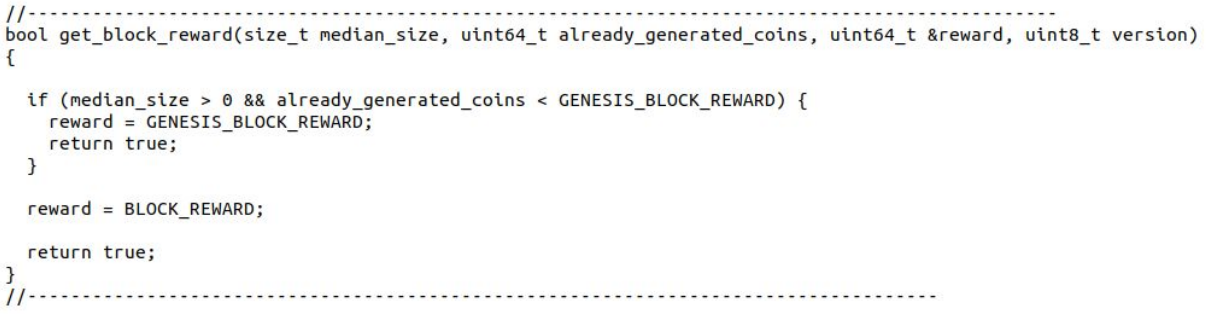
```
Mar 05 11:47:10.458 [notice] Tor 0.3.2.10 (git-0edaa32732ec8930) running on Linux with Libevent 2.1.8-stable, OpenSSL 1.
1.1, Zlib 1.2.11, Liblzma 5.2.2, and Libzstd 1.3.3.
Mar 05 11:47:10.458 [notice] Tor can't help you if you use it wrong! Learn how to be safe at https://www.torproject.org/
download/download#warning
Mar 05 11:47:10.458 [notice] Read configuration file "/etc/tor/torrc".
Mar 05 11:47:10.461 [notice] Scheduler type KIST has been enabled.
Mar 05 11:47:10.461 [notice] Opening Socks listener on 127.0.0.1:9050
Mar 05 11:47:10.000 [notice] Parsing GEOIP IPv4 file /usr/share/tor/geoip.
Mar 05 11:47:10.000 [notice] Parsing GEOIP IPv6 file /usr/share/tor/geoip6.
Mar 05 11:47:10.000 [notice] Bootstrapped 0%: Starting
Mar 05 11:47:11.000 [notice] Starting with guard context "default"
Mar 05 11:47:11.000 [notice] Bootstrapped 80%: Connecting to the Tor network
Mar 05 11:47:11.000 [notice] Bootstrapped 85%: Finishing handshake with first hop
Mar 05 11:47:12.000 [notice] Bootstrapped 90%: Establishing a Tor circuit
Mar 05 11:47:12.000 [notice] Tor has successfully opened a circuit. Looks like client functionality is working.
Mar 05 11:47:12.000 [notice] Bootstrapped 100%: Done
```

Connecting to the Tor Network

Rewards will be sent every 24hrs and will be trackable in a User Interface provided by the RMM. The User Interface will also display your estimated daily reward based on current statistics from the onionoo API. ALL Transactions from the RRMRS will utilize Tor.

Reward Pool Collection

Daily rewards needed by the TRI system will be collected by being part of the Amity Networks core codebase. Currently, Amity’s block reward is 186 coins per block. If approved and the decision is made to move forward with the TRI system, a Hard Fork will be required that will activate splitting the current block reward of 186 into two transactions. One transaction will go to the miner just like a normal block reward and the second will be sent to the RRMRS for collection and processing. The split percentage of the block reward is currently undecided and will be up for discussion.



```
//----------------------------------------------------------------------------------------------
bool get_block_reward(size_t median_size, uint64_t already_generated_coins, uint64_t &reward, uint8_t version)
{

  if (median_size > 0 && already_generated_coins < GENESIS_BLOCK_REWARD) {
    reward = GENESIS_BLOCK_REWARD;
    return true;
  }

  reward = BLOCK_REWARD;

  return true;
}
//-----------------------------------------------------------------------------------
```

Part of the code that determines The Amity Networks current block reward

Conclusion

The Tor Relay Incentive System will be a way for the Amity Network to contribute to the Tor project and its operators and will give Amity a new use case which will hopefully drive adoption and bring more users and miners to the table.

Points Up for Discussion

- Risks of running a Tor Relay or Exit at home
- What percentage of the block reward should be dedicated to TRI System rewards?
- Should TRI System participants be required to run an Open Amity Network Node as well?
- Finally… Wen Moon?