Zcash on Tor Servers Project

Submitted by: xyZcash of zcashtorservers.org

xyzcash@keemail.me

Motivation and overview

See: https://forum.z.cash/t/zcash-on-tor-a-community-funded-proposal/14651

The 'Zcash on Tor' project is an existing and free service for both the Zcash community and Tor users alike.

Our privacy focused service amalgamates high-capacity Zcash peer-to-peer nodes with fast, high-bandwidth Tor servers. The project aims to uphold the core values of the Zcash Foundation, particularly with regard to enabling users to better control their own financial privacy.

The project was started in mid-March 2017 from community donations totalling around $300 and has continued to-date, mainly through ongoing personal contribution.

Our primary motivation is to help solve network correlation issues that can affect regular Zcash users, through the continued provision of our censorship-resistant service and by further empowering and educating users to make the best use of existing software tools. We uphold the individual right to privacy as a basic and fundamental human right.

A grant will primarily enable us to:

1. Maintain our existing Zcash on Tor servers.
2. Establish (at least) 4 new increased capacity (Tier 1) Zcash on Tor .exit servers.
3. Develop and operate a Zcash on Tor .onion enabled mining pool for z_addresses.
4. Set-up (Tor enabled) Zcash Proving key distribution mirrors.
5. Work on supporting documentation, user guides and automated set-up tools.
6. Help to ensure the rights and freedoms of all Zcash on Tor users moving forward.

"Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers." (Art. 19, Universal Declaration of Human Rights, 1948)

Technical approach

We currently host 4 Tor Relays, 1 Tor Exit node and 5 Tor hidden_service client nodes.

Therefore, a total of 10 dedicated *addnode=zcashxxxxxxxxxx.onion* nodes are already made available by our service.

Our public facing Relays can be located via the Tor Atlas:https://atlas.torproject.org/#search/ZcashTor

Each 'Zcash on Tor' IP address runs a full Zcash peer-to-peer node, enabling upwards of 256+ concurrent connections per node (helping to strengthen the network and contributing to a social

good!). 4 new increased capacity (Tier 1) servers will enable us to scale up to thousands of concurrent connections and users.

Details of how to connect with our privacy service can be found via the Zcash Forum: https://forum.z.cash/t/zcash-addnode-tor-hidden-service-onion/13007 - another aim for the project is to improve supporting documentation, user guides and automated set-up tools.

Our example (community) set-up Guide for running Zcash on Tor (Ubuntu / Debian Linux Desktop can be found here: https://forum.z.cash/t/set-up-guide-for-running-zcash-on-tor-ubuntu-debian-linux-desktop/18748 with additional work currently in progress.

Team and background qualifications

xyZcash (a.k.a BitcoinFX) is a long-standing and active member of the Bitcoin and crypto-currency communities. He has been hosting Tor Relay's and Exit nodes for almost 10 years. As a private individual, background qualifications and identity documentation are to be made available to the relevant parties, where deemed to be appropriate and necessary.

Other team members are currently TBD. Consultancy services to be used where appropriate.

Evaluation plan

We will continue to evaluate and provide community updates in regards to our current and future Zcash on Tor service provision. Whilst some metrics (and estimates) can be made available for the approximate number of users and actual bandwidth throughput etc., good anonymity and privacy networks generally do not retain such information by design.

'Live' data can be made available in the form of network maps, service uptime reporting and through anomaly detection / testnet research, where appropriate.

Security considerations

In terms of our operational security - we have partnered with https://tornull.org to limit any potential or actual abuse issues. We already have practical measures in place including firewalls and DDoS protection. See: https://forum.z.cash/t/an-example-zcash-iptables-firewall-for-linux-cloud-servers/8736

We will closely follow all security advisory notifications from both the Zerocoin Electric Coin Company and the Tor Project Inc., in regards to software upgrades and best practices. Our operating systems and cloud services are kept up-to-date with the latest security releases.

From a legal standpoint, as Tor Exit node operators, we are looking to establish a UK based Non-profit ISP (as advised by the Tor Project Inc.) and to perhaps put in place some form of legal defence fund contingency. We already have extensive experience of dealing with and responding to any abuse complaints.

We do not store any Zcash or make any direct transactions via our own servers; as such we are a network of routers operating as common carriers, much like the internet backbone. Our nodes therefore contain no identifiable routing information, or any details of transactions that are not already available on the Zcash blockchain. Our routers maintain no logs whatsoever of any of the Tor traffic and therefore attempts to seize our routers would accomplish nothing.

From a Zcash on Tor user perspective we are keen to work on improving supporting documentation, user guides and automated set-up tools - particularly in regards to users privacy, security and anonymity, as well as choice secure operating systems and procedures.

Schedule

October - November 2017

- Identify appropriate hosting for the new increased capacity (Tier 1) Zcash on Tor .exit servers. - (completed).

- Maintain existing services and perform upgrades where necessary.

November - December 2017

- Set-up our UK registered non-profit ISP.
- Establish and launch (at least) 4 new increased capacity (Tier 1) Zcash on Tor .exit servers.
- Set-up (Tor enabled) Zcash Proving key distribution mirrors.
- Build and launch our full zcashtorservers.org service website.

- Perform a crypto-cannery style ceremony to increase operational security.

December 2017 - January 2018

- Develop and launch our Zcash on Tor .onion enabled mining pool for z_addresses.

- Research and development, Testnet node expansion to 4 nodes, OONI project internet-censorship testing including Zcash related resources. Nodes to be hosted in diverse locations for inclusivity. https://forum.z.cash/t/meet-tazy-our-zcash-on-tor-testnet-node/20398

January 2018 - ongoing

- Work on improving supporting documentation, user guides and automated set-up tools.
- https://forum.z.cash/t/set-up-guide-for-running-zcash-on-tor-ubuntu-debian-linux-desktop/18748
- Build on and facilitate increased community education and outreach.
- Start / facilitate : Zcash on Tor social meet-ups, Zcash on Tor hackathons and/or workshops.
- Continue (and assist) with Zcash privacy research and development, where appropriate.
- Consider integrating additional Zcash on Tor services provision, such as the ORC (Onion Routed Cloud) and/or I2P network connectivity on existing servers.

- Establish and maintain a good social media presence.

- Ensure any donations and in-kind contributions are utilized to maximize the projects potential and maintain the existing service provision to exemplary standards.

Budget and justification

Our full costings analysis is now included within the Financials section of this document.

As a future non-profit ISP we are already operating our free and voluntary service on a tight

personal budget and with some community support. Grant provision will allow the 'Zcash on Tor' project to focus on continuing our privacy research, development and outreach, as well as maintaining and securing existing and new services for the Zcash community and for regular Tor users.

We thank all board members for their consideration.

oooOOOooo

October 2017.

Financials (Amounts in GBP as at 4 October 2017)

ITEM	COST £
Option 1—Maintaining Existing Services for 12 Months	
Personnel 1 part-time worker (myself) 2 half-days x 4 hours x 4 weeks = 32 hours per month (384 hours pa)	4,384 . 00
NB: The above costs are based on a median-to-low full-time salary of a UK Network Administrator @ £21,920pa [*source:* https://www.payscale.com/research/UK/job=Network_Administrator/Salary]	
Equipment Servers and cloud services: Existing servers / upgrades / maintenance for 12 months (including UK VAT @ 20%)	1,583 . 00
Overheads Non-profit company formation and registration: One-time fee Annual fee	105 . 00 75 . 00
Website development and hosting: One-time fee Annual fee	100 . 00 70 . 00
Allowance for insurance, utilities, consumables, office facilities and car use.	100 . 00
Sub Total	6,417 . 00
Contingency @ 10%	642 . 00
TOTAL OPTION 1 … … … … … … … … … … … … … … … … … …	**7,059 . 00**

Financials (Amounts in GBP as at 4 October 2017)

ITEM	COST £
Option 2—As Option 1 with Increased Server Capacity/Throughput	
Personnel 1 part-time worker (myself) 4 half-days x 4 hours x 4 weeks = 64 hours per month (768 hours pa) *NB: The above costs are based on a median-to-low full-time salary of a UK Network Administrator @ £21,920pa* [*source:* https://www.payscale.com/research/UK/job=Network_Administrator/Salary]	8,768 . 00
Equipment Servers and cloud services: Existing servers / upgrades / maintenance for 12 months (including UK VAT @ 20%)	1,583 . 00
4 x new, high-capacity servers for 12 months (including UK VAT @ 20%)	521 . 00
Overheads Non-profit company formation and registration: One-time fee Annual fee	105 . 00 75 . 00
Website development and hosting: One-time fee Annual fee	100 . 00 70 . 00
Allowance for insurance, utilities, consumables, office facilities and car use.	100 . 00
Sub Total	**11,322 . 00**
Contingency @ 10%	1,132 . 00
TOTAL OPTION 2 … … … … … … … … … … … … … … … … … … …	**12,454 . 00**

Financials (Amounts in GBP as at 4 October 2017)

ITEM	COST £
Option 3—As Option 1 With Emphasis on Enhanced R & D	
<u>Personnel</u> 1 part-time worker (myself) 4 half-days x 4 hours x 4 weeks = 64 hours per month (768 hours pa)	8,768 . 00
NB: The above costs are based on a median-to-low full-time salary of a UK Network Administrator @ £21,920pa [*source:* https://www.payscale.com/research/UK/job=Network_Administrator/Salary]	
<u>Equipment</u> Servers and cloud services: Existing servers / upgrades / maintenance for 12 months (including UK VAT @ 20%)	1,583 . 00
Servers for a Tor .onion-enabled mining pool for z_addresses for 12 months (including UK VAT @ 20%)	542 . 00
Development & Research (Testnet expansion included)	452 . 00
<u>Overheads</u> Non-profit company formation and registration: One-time fee Annual fee	105 . 00 75 . 00
Website development and hosting: One-time fee Annual fee	100 . 00 70 . 00
Allowance for insurance, utilities, consumables, office facilities and car use.	100 . 00
Sub Total	**11,795 . 00**
Contingency @ 10%	1,180 . 00
TOTAL OPTION 3 … … … … … … … … … … … … … … … … … … …	<u>**12,975 . 00**</u>

Financials (Amounts in GBP as at 4 October 2017)

ITEM	COST £
Option 4—Maintaining Existing Services for 12 Months with Increased Server Capacity/Throughput and Enhanced R & D	
Personnel 1 part-time worker (myself) 5 half-days x 4 hours x 4 weeks = 80 hours per month (960 hours pa)	10,960 . 00
NB: The above costs are based on a median-to-low full-time salary of a UK Network Administrator @ £21,920pa [source: https://www.payscale.com/research/UK/job=Network_Administrator/Salary]	
Equipment Servers and cloud services: Existing servers / upgrades / maintenance for 12 months (including UK VAT @ 20%)	1,583 . 00
4 x new, high-capacity servers for 12 months (including UK VAT @ 20%)	521 . 00
Servers for a Tor .onion-enabled mining pool for z_addresses for 12 months (including UK VAT @ 20%)	542 . 00
Development & Research (Testnet expansion included)	452 . 00
Overheads Non-profit company formation and registration: One-time fee Annual fee	105 . 00 75 . 00
Website development and hosting: One-time fee Annual fee	100 . 00 70 . 00
Allowance for insurance, utilities, consumables, office facilities and car use.	100 . 00
Sub Total	14,508 . 00
Contingency @ 10%	1,451 . 00
TOTAL OPTION 4 … … … … … … … … … … … … … … … … … …	**15,959 . 00**