Packages - Packaging Request #3344

[gostcoin] Add to repository

2022-09-19 12:15 AM - anonymous

Status:	open	**% Done:**	0%
Priority:	bug		
Assignee:			
Category:			

Description

GOSTCoin (GST) is a digital currency based on blockchain technology. It allows instant payments worldwide with focus on privacy and security of its users.
GOSTCoin is using Invisible Internet (I2P) as a secure network layer.

License: MIT
Git: https://github.com/GOSTSec/gostcoin
Site: https://gostco.in/, http://gostcoin.i2p
AUR package: https://aur.archlinux.org/cgit/aur.git/tree/?h=gostcoin-git

History

#1 - 2022-09-19 05:13 PM - gap

From the readme:

> GOSTCoin uses Soviet and Russian government standard cryptography

This package is not to be trusted.
Governments of all kinds have been known to put backdoors in the "standard" crypto they recommend.

Need I remind everyone of the crypto backdoored by the NSA?
https://en.m.wikipedia.org/wiki/Dual_EC_DRBG

#2 - 2022-09-19 06:09 PM - anonymous

Gostcoin is fork AnonCoin. It was developed by those who created i2pd. The main developers is orignal, R4SAS, villain, hypn. You can contact them in IRC channel ILITA inside i2p network (irc.acetone.i2p over web for example, #gostcoin_ru or #en). The path was choosen to use russian cryptography standards: GOST R 34.10-2012 is a digital signature function (analogue of the ECDSA), GOST R 34.11-2012 is the hashing function (analogue of SHA256/SHA512). If I remember correctly, the random number generator is used from openssl.

#3 - 2022-09-19 07:01 PM - gap

If multiple independent cryptanalysts have deemed a crypto package safe, then that would raise the level of trust we should put in it.
After all, governments need crypto too, and sometimes they do a good job.

However, the fact that GSC not only uses Soviet/Russian crypto instead of other de facto standards like SHA-3, but also brands itself so ostentatiously as such is incredibly suspicious.
In the same way, I wouldn't trust anything branded "USA" and "NSA" with a giant USA-inspired logo, or indeed any patriotic logo, because many governments have been known to put backdoors in crypto.

If the crypto is safe and independently designed, it should have universal application and not need such branding.

#4 - 2022-09-19 07:49 PM - anonymous

I think that there will be no confirmation by independent cryptoanalysts. This is a very unpopular cryptocurrency that operates only inside i2p network. The listed standards of GOST have been developed by government structures that cannot be trust. However, the developers of gostcoin deliberately moved away from the use of the same elliptical curve for all cryptocurrencies. This is considered a feature, not a bug. During the development, of course, the standard and description was studied (sources are open). During the years of existence, there were not found backdoors... As with many programs, everything comes down to trust in the developers.

#5 - 2022-09-19 08:05 PM - anonymous

gap, We will not contain this package at ourselves?

#6 - 2022-09-19 09:49 PM - gap

I would not trust it personally because of the lack of independent audits, the use of Soviet/Russian crypto, and the ostentatious Soviet/Russian branding, which is (quite literally) a big red flag.

bill-auger what are your opinions?
I would not recommended this package is added to Parabola.
It already appears to be libre and in the AUR, so users can already use it if they **really** want to.

#7 - 2022-09-19 09:55 PM - gap

Also, this worries me:
https://en.m.wikipedia.org/wiki/Streebog

> In 2015 Biryukov, Perrin and Udovenko reverse engineered the unpublished S-box generation structure (which was earlier claimed to be generated randomly) and concluded that the underlying components are cryptographically weak.

So from a quick glance it appears that the algorithm is partially a black box, twinned with the typical dishonesty of the Russian Federation?

#8 - 2022-09-21 01:35 PM - bill-auger

gap wrote:

> It already appears to be libre and in the AUR, so users can already use it if they **really** want to.

that is just as true for every packaging request though - as long as packaging requests are being accepted, we can not use that as justification for dismissal

OTOH, just because something is new, hip, and trendy does not mean that parabola needs it either

as usual, it boils down to the desirability/workload ratio - it not obvious yet what this software even is or does - is it a wallet? - a miner? - a transaction processor? - is it any sort of application? - or a plugin for the I2P stack?

more information and more opinions would both be useful

#9 - 2022-09-21 04:15 PM - gap

Judging by the filenames plus the PKGBUILD in the AUR from the first post, it appears to be a wallet interface with an optional Qt GUI:
https://github.com/GOSTSec/gostcoin/tree/master/src

It also appears to have old versions of vendored libraries, so it would probably have to be devendored and updated to support newer versions as native pacman packages instead.
Vendored and outdated dependencies only decrease the level of trust I would put in any project, let alone a crypto wallet which should be always up-to-date and secure.