

Personal storage
Large amounts of money (\$100,000+)
Long-term storage
Infrequently-accessed funds
Technically unskilled users
Expert advisors
Open source

Natural selection	
	fi
Identity spoofing	
racinity opening	
Network exposure	
Under constant attack	
fl	
Internal theft	
Intentional seizure	

**Community review** 



ffl

ffi

Theft

Loss

Betrayal

Availability

Ease of setup fi

Ease of estate planning

fi

Privacy

Signatory collusion

Signatory reliability
Signatory safety

Kidnapping risk

fi

fi

fi

fl

° ffi

•

•

fi • fi

■ fi

° fi

°

° fi

0

•

■ ffi

.

fi

•

•

fi

0

0

fl

0

fl fl

fi

fi

fi fi

fl fl

fi

fl

fl

fi fl

fi

fl

private key
cold storage address
"redemption script"

Perform this protocol using only one quarantined computer

fi

fl

fi

Use existing hardware

fi

fı

ffi

ffi

fl

fi fi

**Setup** fi

Deposit

Withdrawal

Viewing

Maintenance

ffi

ffi

fi

 $\$  echo "everything after the  $\$  could be copy-pasted into a terminal window"

\$

fi

**3** 

## anything that is different recommendation is that you stop and seek help

the

fi

In general, follow the protocol carefully, keep track of what step you are on, and double-check your work

fi

fi

fi

fi

fi

**Windows** 

mac0S

Linux

Windows

mac0S

Linux

Windows > cd \$HOME/Downloads/glacier

macOS \$ cd \$HOME/Downloads/glacier

Linux \$ cd \$HOME/Downloads/glacier

\$ gpg --import \$HOME/Downloads/glacier.asc

fi fi

\$ gpg --verify SHA256SUMS.sig SHA256SUMS

fi

gpg: Signature made Thu Jan 19 13:45:48 2017 PST using RSA key ID
4B43EABO gpg: Good signature from "Glacier Team
<contact@glacierprotocol.org>" [unknown] gpg: WARNING: This key is
not certified with a trusted signature! gpg: There is no indication
that the signature belongs to the owner. Primary key fingerprint:
E1AA EBB7 AC90 C1FE 80FO 1034 9D1B 7F53 4B43 EABO

fi fi fi fi

\$ sha256sum -c SHA256SUMS 2>&1 \$ shasum -a 256 -c SHA256SUMS 2>&1

 $\hbox{Glacier.pdf:} \ \ \hbox{OK glacierscript.py:} \ \ \hbox{OK base} \\ \hbox{58.py:} \ \ \hbox{OK README.md:} \ \ \hbox{OK}$ 

> Get-FileHash -a sha256 Glacier.pdf > cat SHA256SUMS | selectstring -pattern "Glacier.pdf"

fi

fi

fi fi

fi

ffi

fi

fi

Windows macOS

Linux

dc7dee086faabc9553d5ff8ff1b490a7f85c379f49de20c076f11fb6ac7c0f34

fi

ffi

fi fi fi

II II

fi

\$ diskutil unmountDisk USB-device-identifier-here

fi

\$ sudo dd if=ubuntu-16.04.1-desktop-amd64.img.dmg of= USB-device-identifier-here bs=1m

 $\$  sudo dd i f=ubuntu-16.04.1-desktop-amd64.img.dmg of=/dev/disk2 bs=1m

fi

\$ diskutil list

\$ cd \$HOME/Downloads

\$ sudo cmp -n `stat -f %z' ubuntu-16.04.1-desktop-amd64.img.dmg` ubuntu-16.04.1-desktop-amd64.img.dmg USB-device-identifier-here

ubuntu-16.04.1-desktop-amd64.img.dmg /dev/disk2 differ: byte 1, line 1  $\,$ 

Ubuntu

fi

fi fi

fi

Generic Flash Disk (/dev/sda) Kanguru Flash Trust ( /dev/sdb)

fi

\$ cd \$HOME/Downloads

\$ sudo cmp -n `stat -c %s' ubuntu-16.04.1-desktop-amd64.iso` ubuntu-16.04.1-desktop-amd64.iso USB-device-identifier-here

fi

ubuntu-16.04.1-desktop-amd64.iso /dev/sda differ: byte 1, line 1

PC

Mac ~

PC

Mac

fi fi

fi

The Q1 BOOT USB is now eternally quarantined. It should never again be plugged into anything besides the Q1 computer.

fl

fi

fi

fi

\$ gpg --import ~/Downloads/glacier.asc

\$ cd ~/glacier

fi fi

\$ gpg --verify SHA256SUMS.sig SHA256SUMS Expected output (timestamp will vary, but e-mail and fingerprint should match): gpg: Signature made Thu Jan 19 13:45:48 2017 PST using RSA key ID 4B43EABO gpg: Good signature from "Glacier Team <contact@glacierprotocol.org>" [unknown] gpg: WARNING: This key is not certified with a trusted signature! gpg: There is no indication that the signature belongs to the owner. Primary key fingerprint: E1AA EBB7 AC90 C1FE 80FO 1034 9D1B 7F53 4B43

fi fi fi

\$ sha256sum -c SHA256SUMS 2>&1

fi

Glacier.pdf: OK glacierscript.py: OK base58.py: OK README.md: OK

\$ mv ~/.config/nautilus ~/.config/nautilus-bak

fi

\$ sudo mv /var/cache/app-info/xapi an/defaul t /var/cache/appinfo/xapi an/defaul t\_ol d

 $\$  sudo mv /var/cache/app-i nfo/xapi an/defaul t\_ol d /var/cache/app-i nfo/xapi an/defaul t

\$ sudo apt-add-repository universe

\$ sudo apt-add-repository ppa: bitcoin/bitcoin

\$ sudo apt-get update

fi

■ bitcoind

fi

■ qrencode

## ■ zbar-tools

```
$ sudo apt-get install qrencode=3.4.4-1 zbar-tools=0.10
+doc-10ubuntu1 bitcoind
```

fi

```
$ mkdir ~/apps
```

```
$ cp /var/cache/apt/archi ves/*.deb ~/apps
```

fi

apps glacier

fi

```
bi tcoi nd_0. 13. 2-xeni al 1_amd64. deb li bboost-chrono1. 58. 0_1. 58. 0

+dfsg-5ubuntu3. 1_amd64. deb li bboost-program-opti ons1. 58. 0_1. 58. 0

+dfsg-5ubuntu3. 1_amd64. deb li bboost-thread1. 58. 0_1. 58. 0

+dfsg-5ubuntu3. 1_amd64. deb li bdb4. 8++_4. 8. 30-xeni al 2_amd64. deb li bevent-core-2. 0-5_2. 0. 21-stabl e-2_amd64. deb li bevent-pthreads-2. 0-5_2. 0. 21-stabl e-2_amd64. deb li bqrencode3_3. 4. 4-1_amd64. deb

li bsodi um18_1. 0. 8-5_amd64. deb li bzbar0_0. 10+doc-10ubuntu1_amd64. deb

li bzmq5_4. 1. 4-7_amd64. deb qrencode_3. 4. 4-1_amd64. deb zbar-tools_0. 10

+doc-10ubuntu1_amd64. deb
```

base 58. py Glacier. pdf glacierscript. py LICENSE README. md SHA256 SUMS SHA256 SUMS. si g The Q1 APP USB is now eternally quarantined. It should never again be plugged into anything besides the Q1 computer.

fi

fi

fi fi

\$ cd ~/apps \$ sudo dpkg -i \*.deb

\$ cd ~/glacier

\$ chmod +x glacierscript.py



fi

## ~/glacier folder

\$ cd ~/glacier

\$ ./glacierscript.py entropy --num-keys number-of-keys-here

\$ ./glacierscript.py entropy --num-keys 4

Computer entropy #1: f8e1 39f4 8dd2 129c 689c 1cb1 1280 79fe db56 573f Computer entropy #2: c36b 0f66 3344 cd74 1d03 c659 0e7a 92e7 5d1a 663b Computer entropy #3: 6873 b3a9 f1b6 5a06 064a 6e84 7faf f61c 1ef6 5407 Computer entropy #4: 5668 abd2 a7d9 5eb8 f7db 211d fc82 0c15 d4e4 0a04

\$ ./gl aci erscri pt.py

\$ ./gl aci erscri pt. py

5K7 09C6735. MNFkN665YAbb1wWmgs613076. 3i nmvX8fSx7 09A



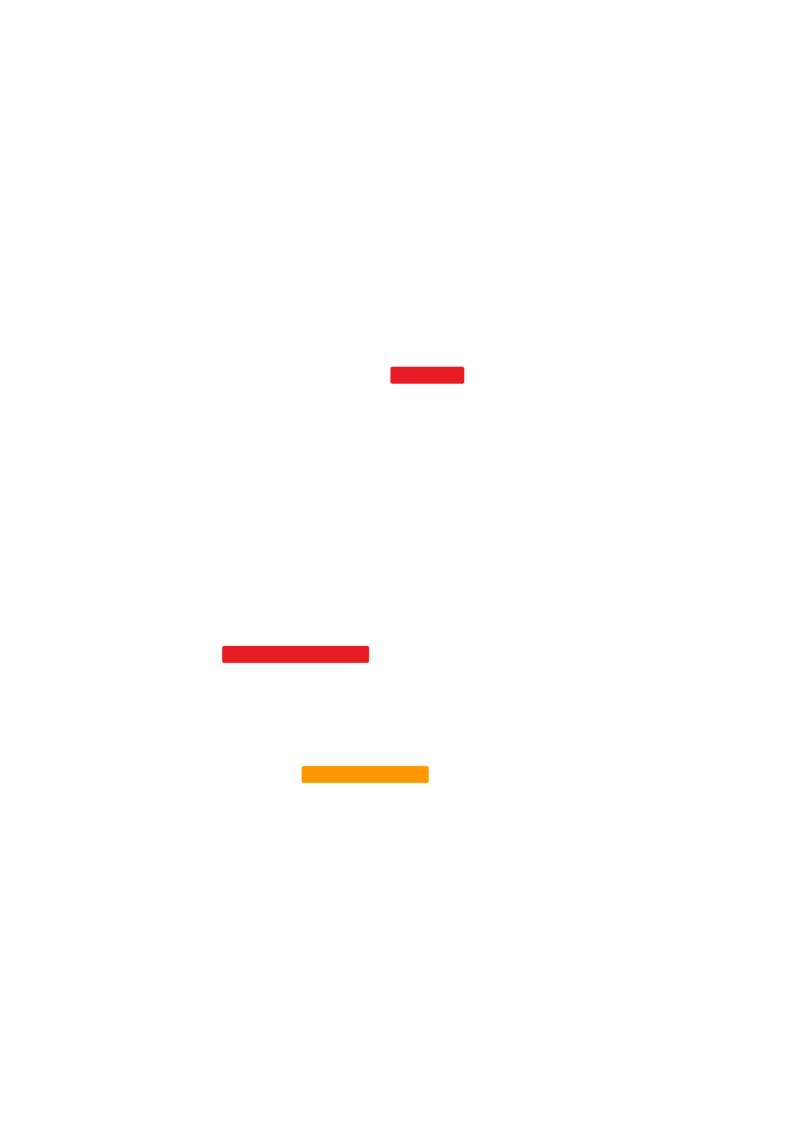
For the private keys and cold storage address, verify ever,

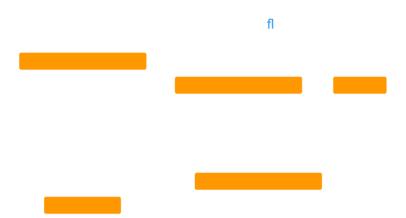
ffi

If there are any discrepancies, do not proceed.



fi



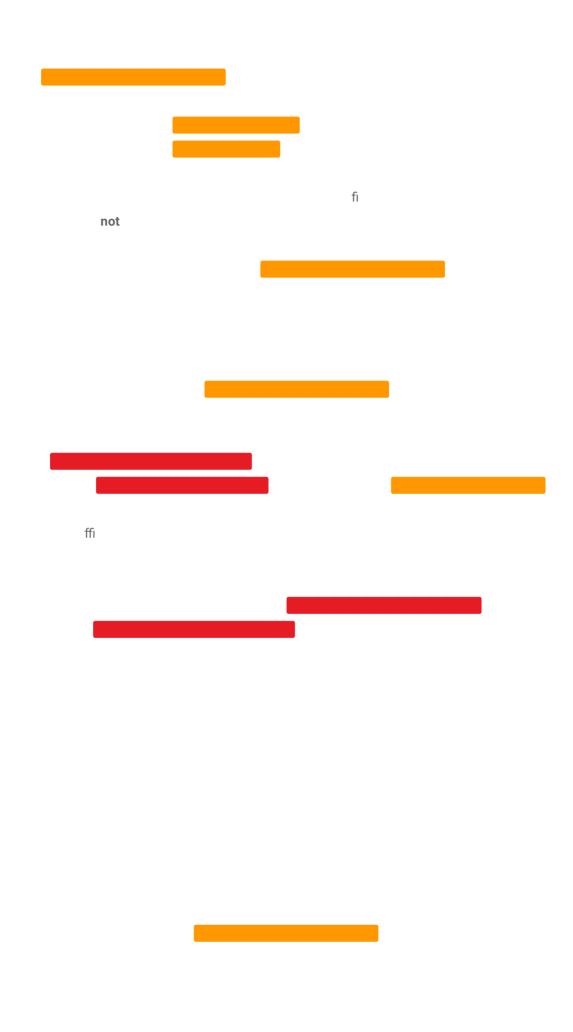


If it does not match, do not proceed



both

\$ sudo shutdown now



fl

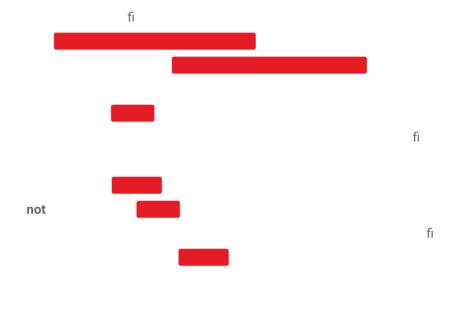
fi

fi

fi fi fl fi

Immediately

ffi



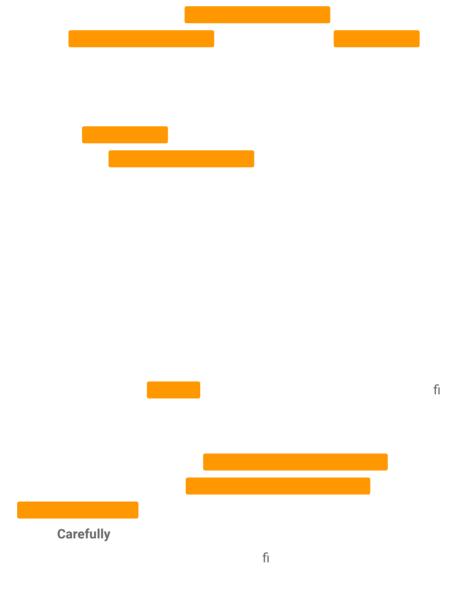
fi

fi

fi

fi

0100000016847105309a8604c7e4f5773d0a16c45248acce057dab62e db0fedc2810d49a401000006b48304502210093e6b4154d42c1bba27c 548a80488673967be32c8de2f11e01a1402a5500e13302203e20874e5d 0af516c902d3b600ee94571a7ce68a14a384dc05d4346e1009fe000121 039fd6f25c87f183260c1d4a3a3ae33a2c06414db4c40d0c2ab76a7192 1fef0939ffffffff01e093040000000001976a914e770a7c13f977478 3e80607f40be4547780315b688ac00000000



{"fastestFee": 100, "hal fHourFee": 100, "hourFee": 70}

ffi

\$ zbarcam

\$QR-Code: 51410421167f7dac2a159bc3957e3498bb6a7c2f1687 4bf1fbbe5b523b3632d2c0c43f1b491f6f2f449ae45c9b0716329 c0c2dbe09f3e5d4e9fb6843af083e222a70a441043704eafafd73 f1c32fafe10837a69731b93c0179fa268fc325bdc08f3bb3056b0 02eac4fa58c520cc3f0041a097232afbe002037edd5ebdab2e493 f18ef19e9052ae

fi

fi

fi

fi

\$ cd ~/gl aci er \$ /gl aci erscri pt. py create-wi thdrawal -data

fi

Sufficient private keys to execute transaction? True Raw signed transaction (hex):

01000000013cd6b24735801ad3d04c40e6da3404278b0d38dbc896df6ae50bf11c3043a49

60000000fda001004730440220199d247cd11c14fa4960a52467e69ca6b77596e94c 14f2

7ba956315f2d1c852302201b6f41ecfc62a1a7c7a423425ab150301cfffc47c1a78a5 bf13

b8232f767e41301483045022100e7ae7e5a77da47d5e622f974683a43d312e72a1eed 329d

4fdbd8fba2c22f84b4022050358fb63cf182e81905417d6e38a2981563495dd00c317 7ee6

50ff7cd2d511a014d0b01524104fe0fcd054a31130749467f07e272426f7dd7a3029a b5b0

76d7285a931bd131d34ed9f28b2cc2fe266aa62c4cada3e82b70a4416966902201c4d

9f7f0425e41044f2ec9f80ef2c4f385f3d27b6167f77236de63548723ba1c90a324f4 ec46

dfd14a2fba5a9c048a5ec310aedfe875d8a254f336e8f7d5d17338d9451dc6f2188c4

efb86098442adc6c3dffd9b0e27fe8e918462469a5ec5363e26920f09facea70b63e4f4d2

736089286d4dd2352ca65016e7d593f105009f9a35c03a2464aa20410451e7f31ea2f 5cb1

4ba76ca20952c1d453fe3a85959ebbefee8912ad6f74c443a03e52ef8a842f890f1ab 2d69

## On the Q2 computer

private keys

fi



Q1 and Q2

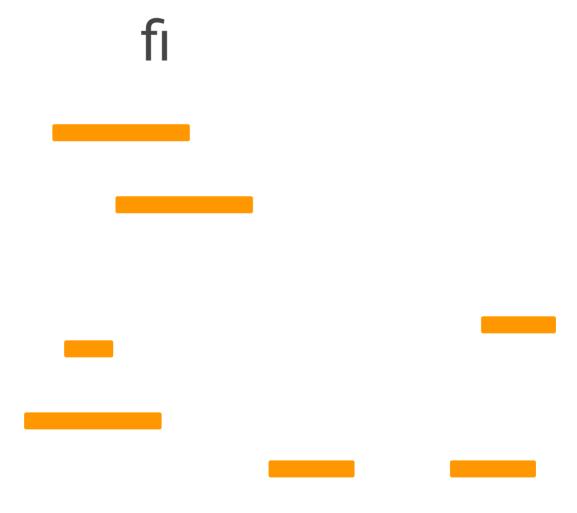
fi

fl
On the Q1 computer

If it does not match, do not proceed

both

\$ sudo shutdown now

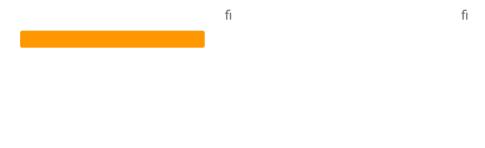


fi fi

six months



fi



fi

Verify GnuPG installation	
Cross-network checksum sourcing	
Quarantined checksum verification	fi
	·
fi  Greater differentiation of quarantined environments	
fl	
Dedicated pair of environments for each private key	
fi	
Deposit transaction verification	fi
Avoid software random number generators	
Faraday cage	

No QR codes

**Purchase factory-new Setup Computers** 

**Use firmware-protected USBs** 

fi

Paper key encryption		
	fi	
Durable storage medium		
High-security vaults		
Geographically distributed storage		
Multiple fund stores		
Unique protocol evecution site	ff	
Unique protocol execution site	III	
Avoid location tracking		
Deliver keys by hand		
Conventional personal security		



fl

O

0

0

0

° fi

°
°

0

0

fi ffi