KEEPER
Cybersecurity Starts Here™

What is the Most Secure Way to Store Cryptocurrencies, like Bitcoin?

Answer: Keeper

Table of Contents

Introduction

Cryptocurrencies, such as Bitcoin, have recently surged in both popularity and value. But the question remains, what is the most secure way to protect and store cryptocurrency?

First, you must understand exactly what a cryptocurrency actually is: A public-private key pair and a public ledger of all transactions called a blockchain.

The public key is given out as a cryptocurrency "address". The private key is used to cryptographically sign messages to prove that you own any balance that may be stored at specific public address. To transfer cryptocurrency from one address to another, the owner uses their private key to cryptographically sign the transaction which is then confirmed and then incorporated into the blockchain. By examining the blockchain, anyone can determine how much currency is stored at a specific address, or at any point of time in the past.

A bitcoin public key (or address) looks like this

1HTaYTjeYwLexmmbsbNLieo2NTReS7UUzk

While the corresponding private key would look something like this example

Kzbw8ReJobEU9KmwucfkQUcvY7aQomVDxZzcuvwLCMSoYXaWqEU

The public key can be freely given out in order to facilitate transactions to your wallet, while the private key must be kept secure.

Where Do People Typically Keep Cryptocurrency?

The private key makes it possible to initiate transfers of cryptocurrency from a particular address. Keeping the cryptocurrency private key secure is essential to keeping your cryptocurrency balances secure. Anyone on the internet with access to the private key can initiate transactions of any balance held in the corresponding public address.

Cryptocurrency private key is typically stored in these various ways:

- An online wallet service
- A wallet application running on the end-user's device
- A wallet file stored in offline electronic media
- Printed on a piece of paper and stored in a secure location

What are the Risks Storing Cryptocurrency this Way?

Many online cryptocurrency wallets suffer from a major flaw: The wallet provider must have access to your wallet private key in order to initiate transactions on your behalf. It is impossible for online wallet services to initiate blockchain transactions without the secret key. Giving the secret key to an online wallet means that you must trust the online wallet to keep your wallet secret key secure. Even worse, the secret key must be kept online and accessible for the wallet to initiate transactions—where vulnerabilities, such as Meltdown, can be used by cybercriminals to potentially steal cryptocurrency private keys.

What if I Lose My Private Key?

Private keys are obviously far too long and complex for most people to remember. It is common for people to lose their private key. If it wasn't stored in a safe place such as a password manager or secure wallet, you're out of luck. Without your private key, your access to your cryptocurrency will be denied and redeeming it for goods, services or cash will be impossible.

Other online cryptocurrency services require users to transfer cryptocurrency to a wallet controlled by the service. Users must ultimately trust the wallet service to track how much cryptocurrency is stored in their account. In many ways, these services operate like a traditional bank. Account balances for each user must be kept online and accessible – making them potentially vulnerable to manipulation by malicious employees, cybercriminals, or seizure by government entities. Many of the security and anonymity benefits of holding funds in cryptocurrency are lost by using online cryptocurrency wallet services.

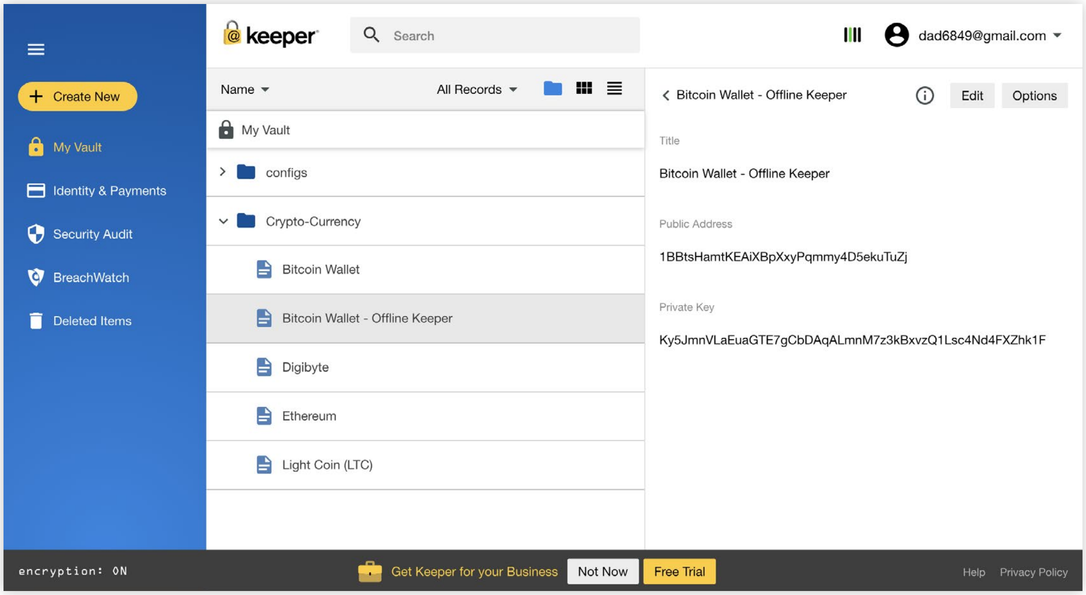
Recent history is rife with examples of fraud and hacks of online cryptocurrency wallets and cryptocurrency services. Cryptocurrency will continue to grow as a target for cybercriminals as it increases in value and interest.

How Can You Protect Your Cryptocurrency From Cybercriminals?

Many of the techniques used to secure passwords and login credentials can be used to secure cryptocurrency private keys. It is commonly agreed that the best way to protect your cryptocurrency from cybercriminals is by use of cold or offline storage, that is, either on a printed paper wallet or electronic storage (hard drive, SSD, flash drive) that is not connected to the internet. The problem that arises from offline wallets or paper wallets is physical security and accessibility. Anyone with physical access to the offline wallet potentially has access to the currency stored in that wallet, and thus it must be protected and secured like any other valuable physical asset, such as being stored in a bank safety deposit box. A Bitcoin secret key stored on a flash drive or printed on paper wallet sitting in a safety deposit box thousands of miles away is not conveniently accessible.

What is the Best Solution for Securely Storing Cryptocurrency?

Keeper was created to securely store, backup, and synchronize passwords and private keys, and thus is a great option for backing up and storing cryptocurrency. Keeper uses zero-knowledge AES 256-bit encryption - the keys used to encrypt and decrypt the passwords or keys stored in your Keeper vault are derived on your device from your master password. Since the keys are derived on and never leave your device, neither Keeper, nor anyone else, has the ability to decrypt any data stored within Keeper.



Title

Bitcoin Wallet - Offline Keeper

Public Address

1BBtsHamtKEAiXBpXxyPqmmy4D5ekuTuZj

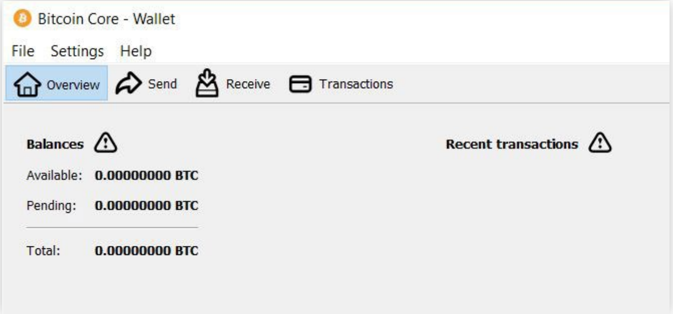
Private Key

Ky5JmnVLaEuaGTE7gCbDAqALmnM7z3kBxvzQ1Lsc4Nd4FXZhk1F

Keeper offers many of the convenience benefits of online wallets and online cryptocurrency services while allowing you retain the security benefits of an offline wallet by keeping control over your cryptocurrency private keys. By backing up or storing your cryptocurrency wallet using a product with zero-knowledge architecture, like Keeper, cryptocurrency wallets, keys, or credentials can be securely backed-up or synchronized across multiple devices.

How Can You Export Your Private Key?

If you already have a fully synchronized wallet that you would like to store in your Keeper vault, you can do so easily by extracting your private keys from your wallet. This example shows how to extract a private key from a Bitcoin Core wallet. Note that many cryptocurrency wallets (Including Litecoin, Dogecoin, Digibyte, etc) share the same interfaces and commands. The wallet and corresponding address that you will see in the article was generated specifically for this test and contains no BTC balance. The examples that you will see are real addresses and real private keys that theoretically anyone could use now that the private keys have been divulged in this article.



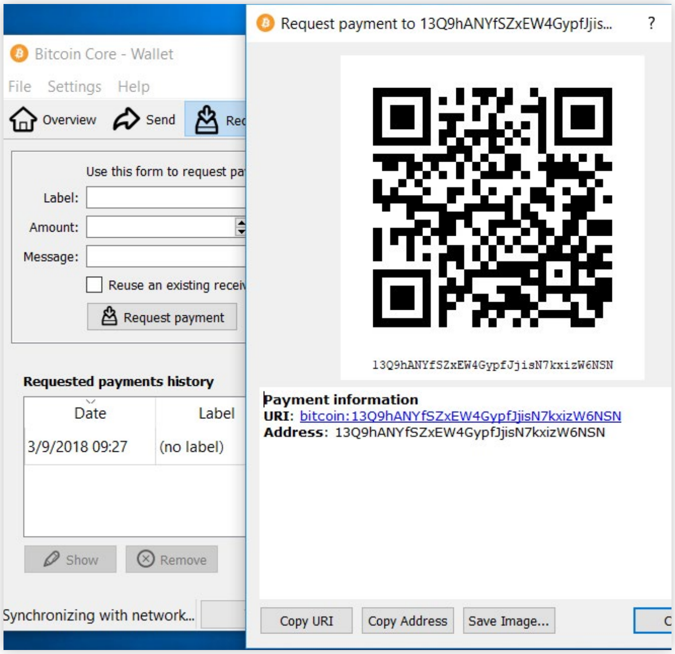
Balances

Available: 0.00000000 BTC

Pending: 0.00000000 BTC

Total: 0.00000000 BTC

First, click the “Receive” button and then next screen click the “Request Payment” button. This will generate a new bitcoin address and private key. The bitcoin address will be displayed along with a QR code representation of the bitcoin address. This address would be given out to anyone from which you wish to receive a bitcoin payment.



Requested payments history

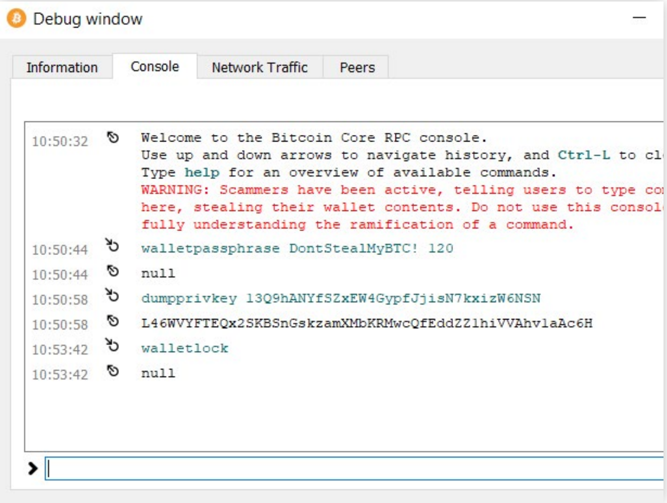
Date	Label
3/9/2018 09:27	(no label)

13Q9hANYfSZxEW4GypfJjisN7kxizW6NSN

Payment information
URI: bitcoin:13Q9hANYfSZxEW4GypfJjisN7kxizW6NSN
Address: 13Q9hANYfSZxEW4GypfJjisN7kxizW6NSN

Extracting the private key may be done through the console. First, copy your address from the Request payment window (click the “Copy Address” button).

From the “Help” menu, select the debug window. In the debug window select the console tab. Type the command “dumpprivkey” and then a space and paste the address. For example, if we want to extract the private key for the address “13Q9hANYfSZxEW4GypfJjisN7kxizW6NSN”, the command would be “dumpprivkey 13Q9hANYfSZxEW4GypfJjisN7kxizW6NSN”.



```
10:50:32    Welcome to the Bitcoin Core RPC console.
            Use up and down arrows to navigate history, and Ctrl-L to cl
            Type help for an overview of available commands.
            WARNING: Scammers have been active, telling users to type co
            here, stealing their wallet contents. Do not use this consol
            fully understanding the ramification of a command.
10:50:44    walletpassphrase DontStealMyBTC! 120
10:50:44    null
10:50:58    dumpprivkey 13Q9hANYfSZxEW4GypfJjisN7kxizW6NSN
10:50:58    L46WVYFTEQx2SKBSnGskzamXMbKRMwcQfEddZZ1hiVVAhvlaAc6H
10:53:42    walletlock
10:53:42    null
```

The dumpprivkey command can only be performed on an unlocked wallet. It is highly recommended that you ALWAYS lock your wallet when not in use. If your wallet is locked, it will be necessary to use the walletpassphrase command to unlock your wallet. Once your wallet is unlocked you can use the dumpprivkey command to extract the private key for the specified address. If you have multiple addresses with balances in your wallet, you must perform dumpprivkey commands for each address to display the corresponding private key for each. When you have finished extracting private keys, use the walletlock command to lock your wallet.

Business Sales

Americas & APAC	+1 312 829 2680
United Kingdom	+44 20 3405 8853
Germany & DACH	+49 89 143772993
Ireland	+353 21 229 6020
EMEA	+353 21 229 6011
Netherlands	+31 20 262 0932
Iberia & Italy	+34 919 01 65 13
Sweden & Nordics	+46 8 403 049 28

Support

Consumer	+1 312 971 5702
Business (Americas & APAC)	+1 312 226 4782
Business (EMEA)	+353 21 229 6019

keepersecurity.com **sales@keepersecurity.com**