OECD International Academy for Tax Crime Investigation

Anti-Money Laundering: Current Trends, Prosecutions, and the Challenges around Cryptocurrencies

OECD

Paper Wallets

Paper Wallets

- May be created for any cryptocurrency.
- **Contain the private key** for a virtual asset address or account.
- Often contain both an Address (or Account) and a Private Key.
- May contain an encrypted private key
  - The user will need to enter a password or passphrase when using the wallet.
- Invented by Peter Kroll (Canadian)
  - Bitaddress.org

The Bitcoin Game #56: Paper Wallet Inventor Peter Kroll

https://www.youtube.com/watch?v=G2_Y842YdXE

Why would you want to use a paper wallet?

- You can create wallets for every search location and provide them to searchers to use for seizure.
  - **You can provide the searchers with only the addresses to seize to and keep the keys separately.**
- You secure assets offline (cold storage)
- You can distribute sets of keys to multiple individuals
  - Managers
  - Legal
  - Seized property management

If you locate a paper wallet on search

It is imperative to limit the number of people who see the paper wallet to as few as possible.

Anyone with access to the private key recorded on the paper can control the cryptocurrency.

If you locate a paper wallet on a search

1. **Secure the wallet immediately**
   - Use "security envelopes"
2. **Limit access to the private key**
3. **Seize & secure the assets held in the wallets as soon as possible.**

Note: You can scan paper wallet addresses with many computer or cell phone wallets and determine the funds they hold.

PAPER WALLET GENERATORS

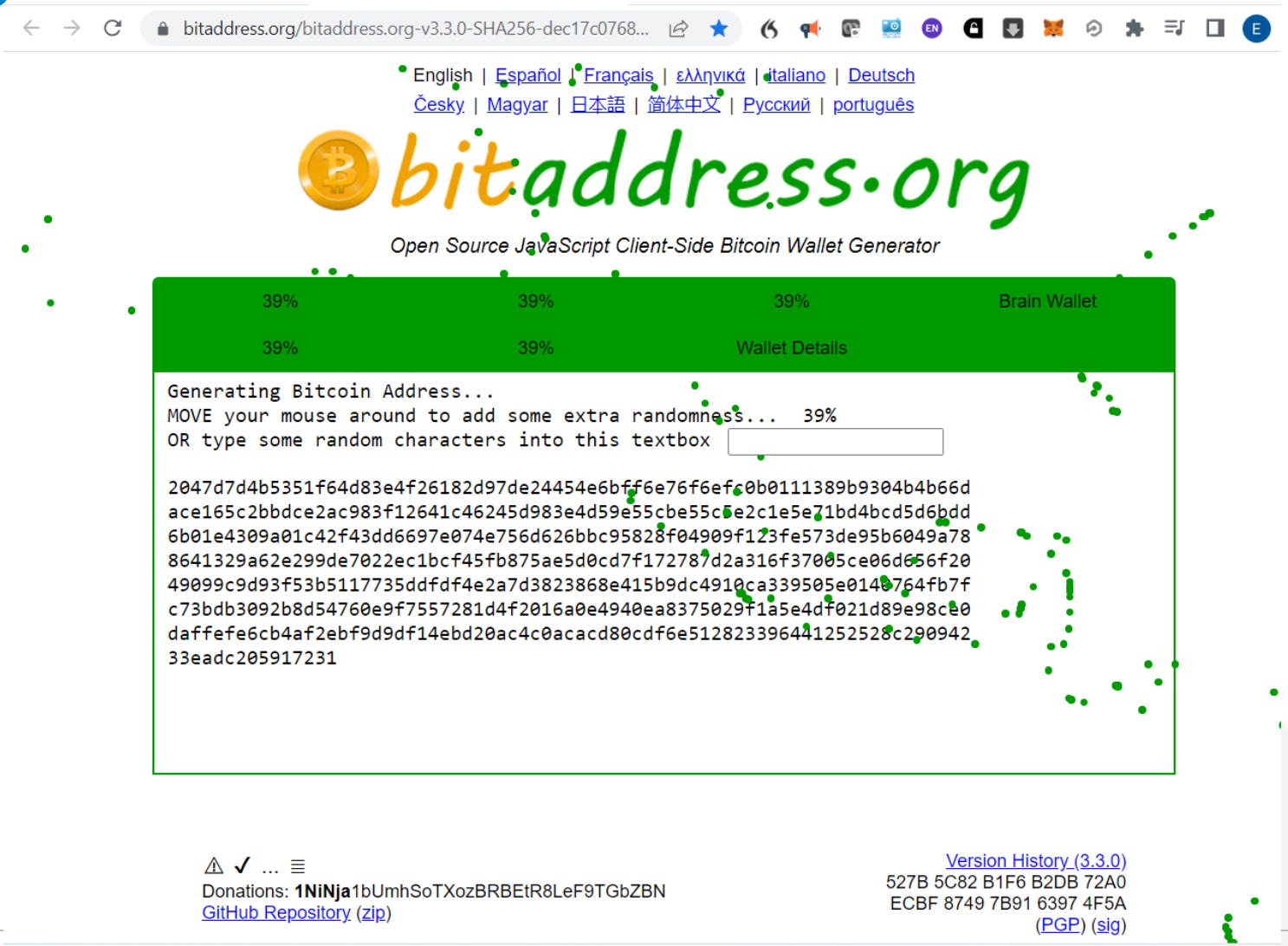
Web Page Paper Wallet Generators

1. Generate a random 256 bit number
2. Generate a private key from the random number
3. Generate an address from the private key

- Web based wallet generators use Java Code embedded in the web page to create wallets.
- You can download the web page and generate wallets offline.

```
    GitHub Repository: https://github.com/pointbiz/bitaddress.org
    -->

    <title>bitaddress.org</title>
    <meta charset="utf-8">

    <script type="text/javascript">
/*!
* Crypto-JS v2.5.4  Crypto.js
* http://code.google.com/p/crypto-js/
* Copyright (c) 2009-2013, Jeff Mott. All rights reserved.
* http://code.google.com/p/crypto-js/wiki/License
*/
if (typeof Crypto == "undefined" || !Crypto.util) {
    (function () {

        var base64map = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/";

        // Global Crypto object
        var Crypto = window.Crypto = {};

        // Crypto utilities
        var util = Crypto.util = {

            // Bit-wise rotate left
            rotl: function (n, b) {
                return (n << b) | (n >>> (32 - b));
            },

            // Bit-wise rotate right
            rotr: function (n, b) {
                return (n << (32 - b)) | (n >>> b);
            },

            // Swap big-endian to little-endian and vice versa
            endian: function (n) {

```

Your mouse movements are used to generate a random number



bitaddress.org

Open Source JavaScript Client-Side Bitcoin Wallet Generator

Single Wallet | Paper Wallet | Bulk Wallet | Brain Wallet

Vanity Wallet | Split Wallet | Wallet Details

Generate New Address | Print

Bitcoin Address | **Private Key**

SHARE

SECRET

1PkFzCFvizdA5ePkrP4PzD1hkVGpFKJX6c

L3axA9ccqV4t9Gs1miC4UpVJgxR2drnvVFcY58QfQVZoKP19uxsk

A Bitcoin wallet is as simple as a single pairing of a Bitcoin address with its corresponding Bitcoin private key. Such a wallet has been generated for you in your web browser and is displayed above.

To safeguard this wallet you must print or otherwise record the Bitcoin address and private key. It is important to make a backup copy of the private key and store it in a safe location. This site does not have knowledge of your private key. If you are familiar with PGP you can download this all-in-one HTML page and check that you have an authentic version from the author of this site by matching the SHA256 hash of this HTML with the SHA256 hash available in the signed version history document linked on the footer of this site. If you leave/refresh the site or press the "Generate New Address" button then a new private key will be generated and the previously displayed private key will not be retrievable. Your Bitcoin private key should be kept a secret. Whomever you share the private key with has access to spend all the bitcoins associated with that address. If you print your wallet then store it in a zip lock bag to keep it safe from water. Treat a paper wallet like cash.

Add funds to this wallet by instructing others to send bitcoins to your Bitcoin address.

Check your balance by going to blockchain.info or blockexplorer.com and entering your Bitcoin address.

Spend your bitcoins by going to blockchain.info and sweep the full balance of your private key into your account at their website. You can also spend your funds by downloading one of the popular bitcoin p2p clients and importing your private key to the p2p client wallet. Keep in mind when you import your single key to a bitcoin p2p client and spend funds your key will be bundled with other private keys in the p2p client wallet. When you perform a transaction your change will be sent to another bitcoin address within the p2p client wallet. You must then backup the p2p client wallet and keep it safe as your remaining bitcoins will be stored there. Satoshi advised that one should never delete a wallet.

You can create "Vanity" addresses (Addresses containing specific words)

Open Source JavaScript Client-Side Bitcoin Wallet Generator

Single Wallet | Paper Wallet | Bulk Wallet | Brain Wallet

Vanity Wallet | Split Wallet | Wallet Details

Step 1 - Generate your "Step1 Key Pair" [Generate]

Step 2 - Calculate your Vanity Wallet

Enter Your Part Private Key (generated in Step 1 above and previously saved):
[NOTE: this input box can accept a public key or private key]

Enter Pool Part Private Key (from Vanity Pool):
[NOTE: this input box can accept a public key or private key]

Add (•) Multiply ( )

[Calculate Vanity Wallet]

⚠ ✓ ✓ ≡
Donations: **1NiNja**1bUmhSoTXozBRBEtR8LeF9TGbZBN
GitHub Repository (zip)

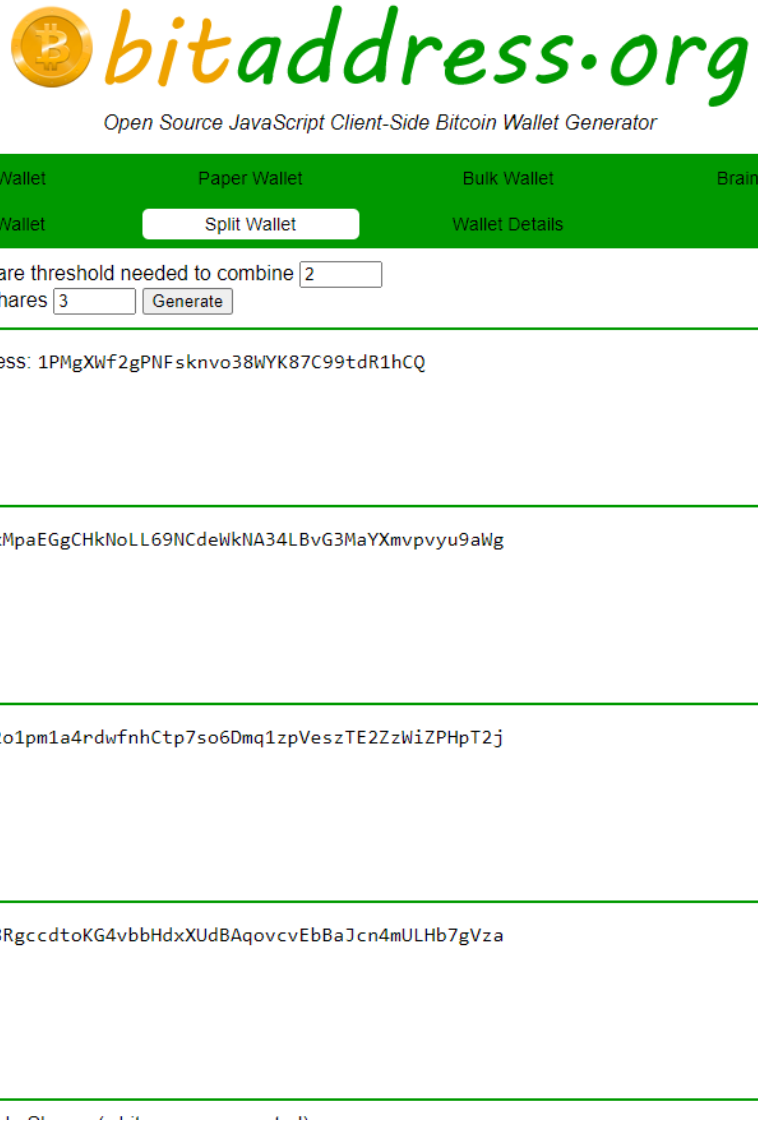
Version History (3.3.0)
527B 5C82 B1F6 B2DB 72A0
ECBF 8749 7B91 6397 4F5A
(PGP) (sig)

You can create a “Brain Wallet”

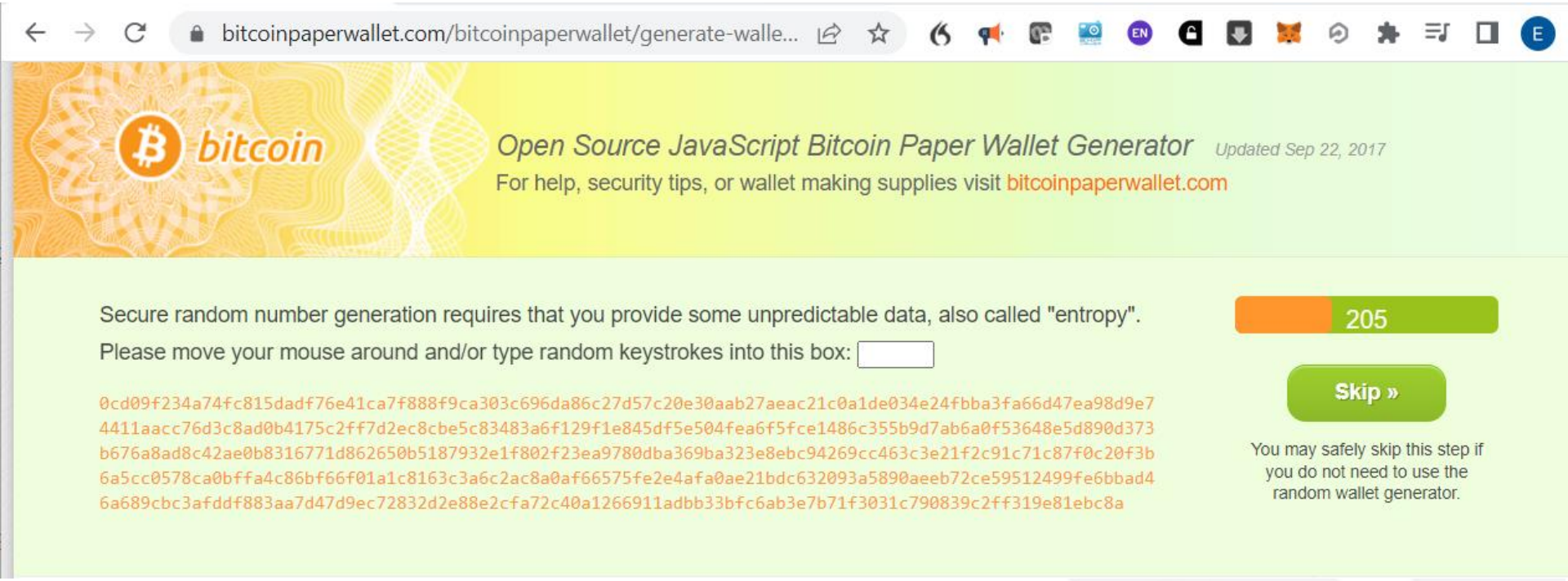
(A wallet where the private key is generated from a pass phrase)

“She walks in beauty like the night.”

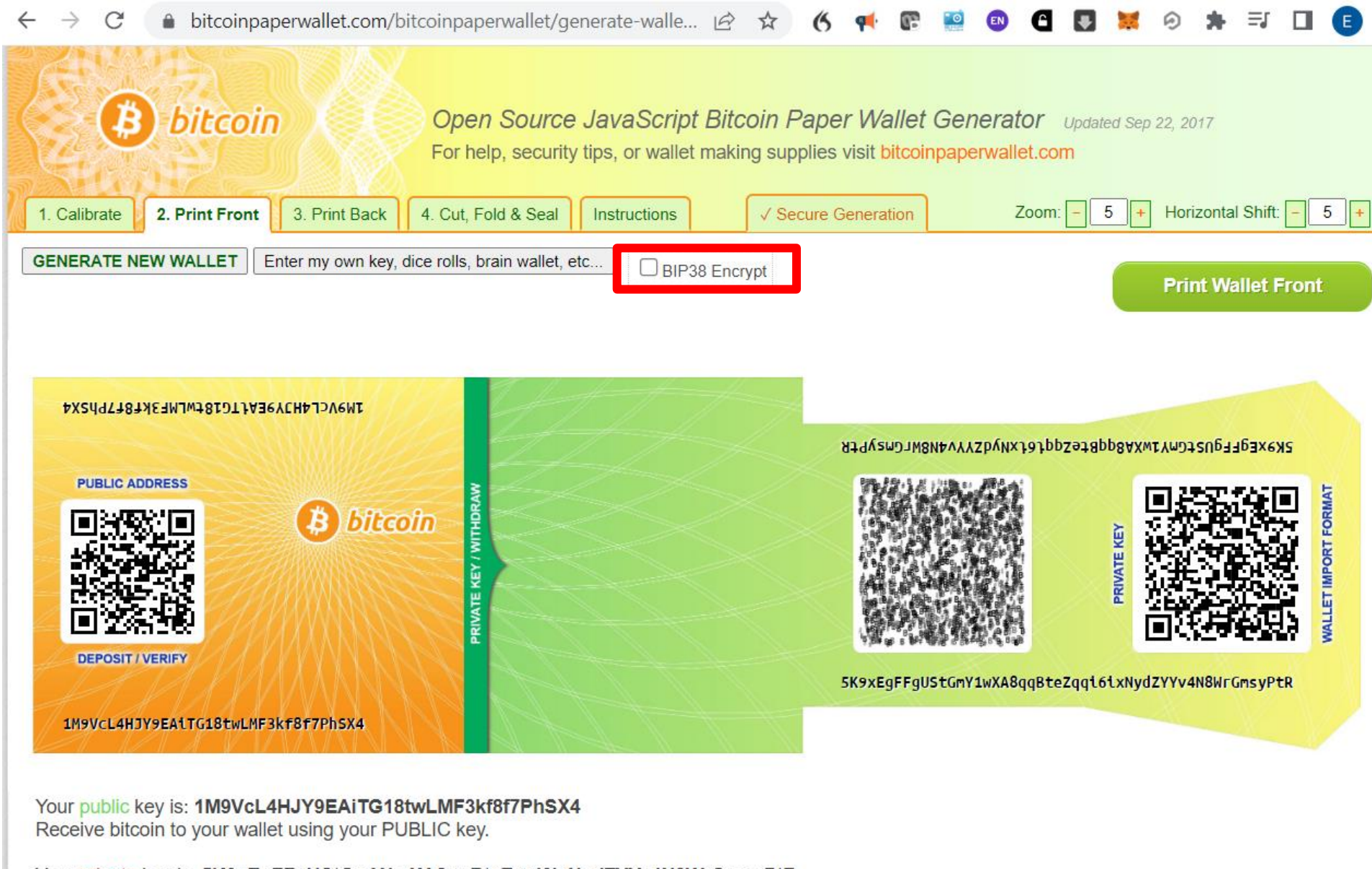
You can create a “Split” wallet (i.e. a Multisignature wallet)

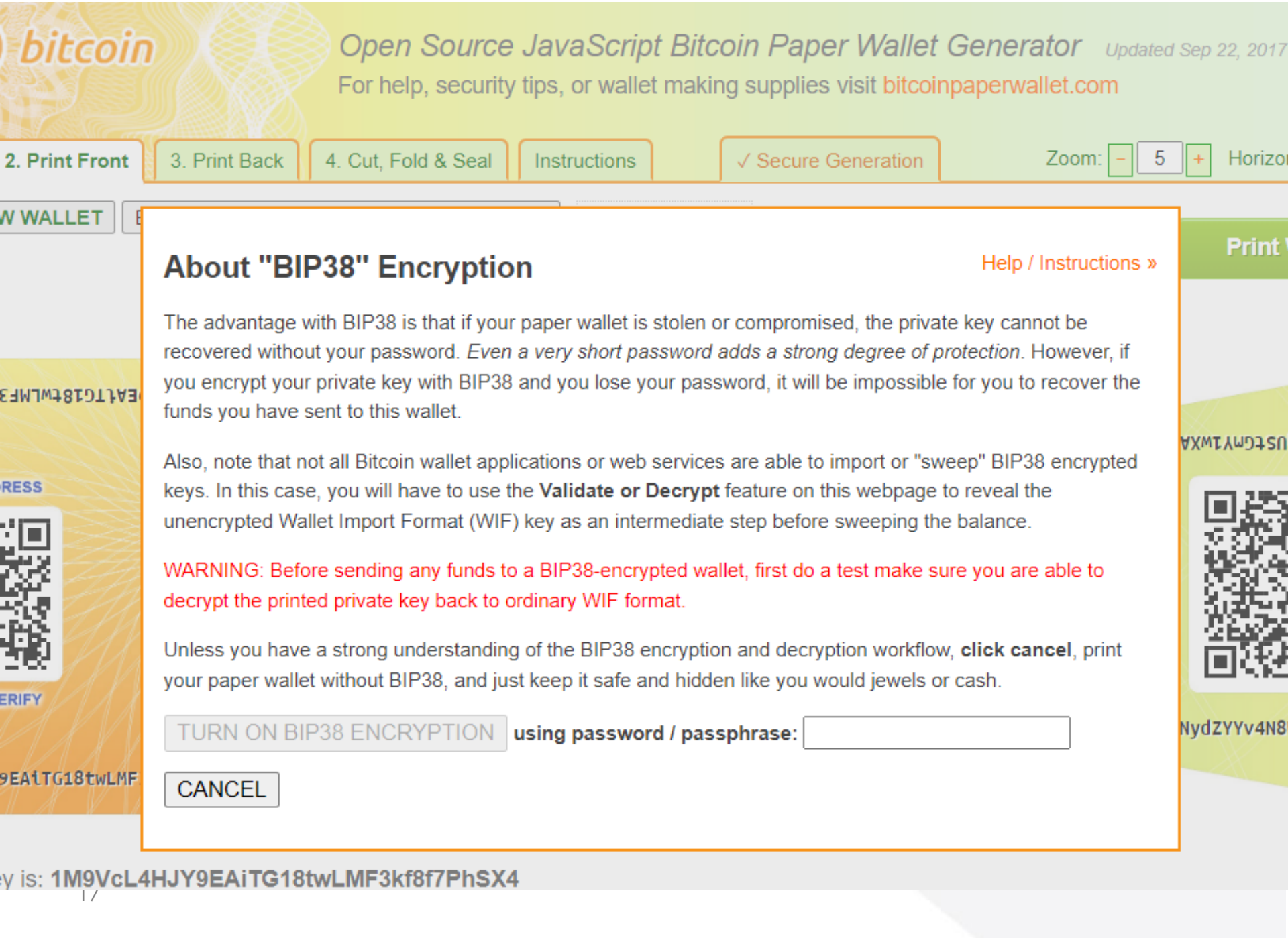


BitcoinPaperWallet.com



Encrypted Wallets




bitcoin
Open Source JavaScript Bitcoin Paper Wallet Generator
Updated Sep 22, 2017
For help, security tips, or wallet making supplies visit bitcoinpaperwallet.com
2. Print Front
3. Print Back
4. Cut, Fold & Seal
Instructions
✓ Secure Generation
Zoom:
5
W WALLET
Print
About "BIP38" Encryption
Help / Instructions »
The advantage with BIP38 is that if your paper wallet is stolen or compromised, the private key cannot be recovered without your password. Even a very short password adds a strong degree of protection. However, if you encrypt your private key with BIP38 and you lose your password, it will be impossible for you to recover the funds you have sent to this wallet.
Also, note that not all Bitcoin wallet applications or web services are able to import or "sweep" BIP38 encrypted keys. In this case, you will have to use the Validate or Decrypt feature on this webpage to reveal the unencrypted Wallet Import Format (WIF) key as an intermediate step before sweeping the balance.
WARNING: Before sending any funds to a BIP38-encrypted wallet, first do a test make sure you are able to decrypt the printed private key back to ordinary WIF format.
Unless you have a strong understanding of the BIP38 encryption and decryption workflow, click cancel, print your paper wallet without BIP38, and just keep it safe and hidden like you would jewels or cash.
TURN ON BIP38 ENCRYPTION
using password / passphrase:
CANCEL
y is: 1M9VcL4HJY9EAiTG18twLMF3kf8f7PhSX4

About "BIP38" Encryption

Help / Instructions »

The advantage with BIP38 is that if your paper wallet is stolen or compromised, the private key cannot be recovered without your password. *Even a very short password adds a strong degree of protection*. However, if you encrypt your private key with BIP38 and you lose your password, it will be impossible for you to recover the funds you have sent to this wallet.

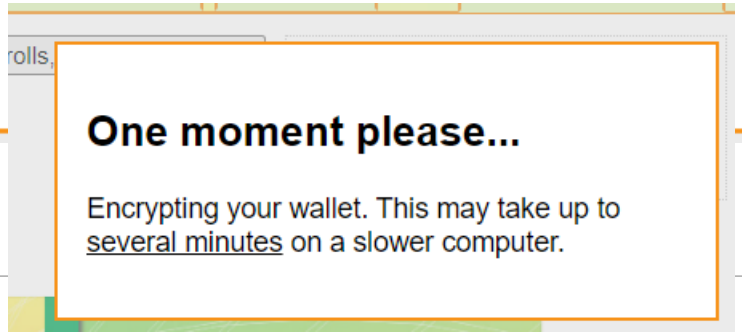
Also, note that not all Bitcoin wallet applications or web services are able to import or "sweep" BIP38 encrypted keys. In this case, you will have to use the **Validate or Decrypt** feature on this webpage to reveal the unencrypted Wallet Import Format (WIF) key as an intermediate step before sweeping the balance.

WARNING: Before sending any funds to a BIP38-encrypted wallet, first do a test make sure you are able to decrypt the printed private key back to ordinary WIF format.

Unless you have a strong understanding of the BIP38 encryption and decryption workflow, **click cancel**, print your paper wallet without BIP38, and just keep it safe and hidden like you would jewels or cash.

TURN ON BIP38 ENCRYPTION **using password / passphrase:** This is my very secure passp

CANCEL



Online paper wallet generators

Not secure

- Who is hosting the web page and potentially intercepting your private key?
- Did you to go the correct URL?
- Have you verified the code on the web page?
- Are there computational weaknesses?

Some law enforcement agencies have written their own paper wallet generators.

PAPER WALLET EXERCISE

Paper Wallet Exercise

1. Create a paper wallet using either Bitaddress.org or Bitcoinpaperwallet.com
   - https://www.bitaddress.org/bitaddress.org-v3.3.0-SHA256-dec17c07685e1870960903d8f58090475b25af946fe95a734f88408cef4aa194.html
   - https://bitcoinpaperwallet.com/bitcoinpaperwallet/generate-wallet.html

2. Print the paper wallet as a PDF file and save it to your computer.