



OECD International Academy for Tax Crime Investigation

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



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

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.

```
45 GitHub Repository: https://github.com/pointbiz/bitaddress.org
46 -->
47
48 <title>bitaddress.org</title>
49 <meta charset="utf-8">
50
51 <script type="text/javascript">
52 /**
53 * Crypto-JS v2.5.4  Crypto.js
54 * http://code.google.com/p/crypto-js/
55 * Copyright (c) 2009-2013, Jeff Mott. All rights reserved.
56 * http://code.google.com/p/crypto-js/wiki/License
57 */
58 if (typeof Crypto == "undefined" || !Crypto.util) {
59     (function () {
60
61         var base64map = "ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/";
62
63         // Global Crypto object
64         var Crypto = window.Crypto = {};
65
66         // Crypto utilities
67         var util = Crypto.util = {
68
68             // Bit-wise rotate left
69             rotl: function (n, b) {
70                 return (n << b) | (n >>> (32 - b));
71             },
72
73             // Bit-wise rotate right
74             rotr: function (n, b) {
75                 return (n << (32 - b)) | (n >>> b);
76             },
77
78             // Swap big-endian to little-endian and vice versa
79             endian: function (n) {
80
81
```

Your mouse movements are used to generate a random number

The screenshot shows the bitaddress.org website, a client-side Bitcoin wallet generator. The page has a green header with the text "bitaddress.org" and "Open Source JavaScript Client-Side Bitcoin Wallet Generator". Below the header, there is a green bar with the text "Generating Bitcoin Address..." and "MOVE your mouse around to add some extra randomness... 39%". There is also a text input box with the placeholder "OR type some random characters into this textbox". A large green box contains a long string of random characters: 2047d7d4b5351f64d83e4f26182d97de24454e6bf6e76f6efc0b0111389b9304b4b66d ace165c2bbdce2ac983f12641c46245d983e4d59e55cbe55c5e2c1e5e71bd4bcd5d6bdd 6b01e4309a01c42f43dd6697e074e756d626bbc95828f04909f123fe573de95b6049a78 8641329a62e299de7022ec1bcf45fb875ae5d0cd7f172787d2a316f37005ce06d656f20 49099c9d93f53b5117735ddf4e2a7d3823868e415b9dc4910ca339505e0148764fb7f c73bdb3092b8d54760e9f7557281d4f2016a0e4940ea8375029f1a5e4df021d89e98ce0 daffefef6cb4af2ebf9d9df14ebd20ac4c0acacd80cdf6e512823396441252528c290942 33eadc205917231

At the bottom, there are links for "Version History (3.3.0)", "527B 5C82 B1F6 B2DB 72A0", "ECBF 8749 7B91 6397 4F5A", and "(PGP) (sig)".



Single Wallet

Paper Wallet

Bulk Wallet

Brain Wallet

Vanity Wallet

Split Wallet

Wallet Details

Generate New Address

Print

Bitcoin Address

Private Key



SHARE

1PkFzCFvizdA5ePkrP4PzD1hkVGpFKJX6c



SECRET

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)



Single Wallet	Paper Wallet	Bulk Wallet	Brain Wallet
<input type="button" value="Vanity Wallet"/>	<input type="button" value="Split Wallet"/>	<input type="button" value="Wallet Details"/>	
<p>Step 1 - Generate your "Step1 Key Pair" <input type="button" value="Generate"/> +</p>			
<p>Step 2 - Calculate your Vanity Wallet +</p> <p>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] <input type="text"/></p> <p>Enter Pool Part Private Key (from Vanity Pool): [NOTE: this input box can accept a public key or private key] <input type="text"/></p> <p>Add <input checked="" type="radio"/> Multiply <input type="radio"/></p> <p><input type="button" value="Calculate Vanity Wallet"/></p>			



Donations: **1NiNja1bUmhSoTxozBRBEtR8LeF9TGbZBN**
[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.”



bitaddress.org

Open Source JavaScript Client-Side Bitcoin Wallet Generator

Single Wallet

Paper Wallet

Bulk Wallet

Brain Wallet

Vanity Wallet

Split Wallet

Wallet Details

Enter Passphrase:

Show?

Print

Confirm Passphrase:

Algorithm: SHA256(passphrase)

Compressed address?

Warning: Choosing a strong passphrase is important to avoid brute force attempts to guess your passphrase and steal your bitcoins.



Bitcoin Address:

1EJnh4hTkYdT6BezrGByMwMVXjA8bwsWK



Private Key (Wallet Import Format):

5JUteWRieAkLCB9DCMlqZt85j8jhS2qSCYa3Y3ehvUVP9w6SZ1L

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



Open Source JavaScript Client-Side Bitcoin Wallet Generator

Single Wallet Paper Wallet Bulk Wallet Brain Wallet

Vanity Wallet Split Wallet Wallet Details

Minimum share threshold needed to combine Number of shares

Bitcoin Address: 1PMgXWf2gPNFsknvo38WYK87C99tdR1hCQ

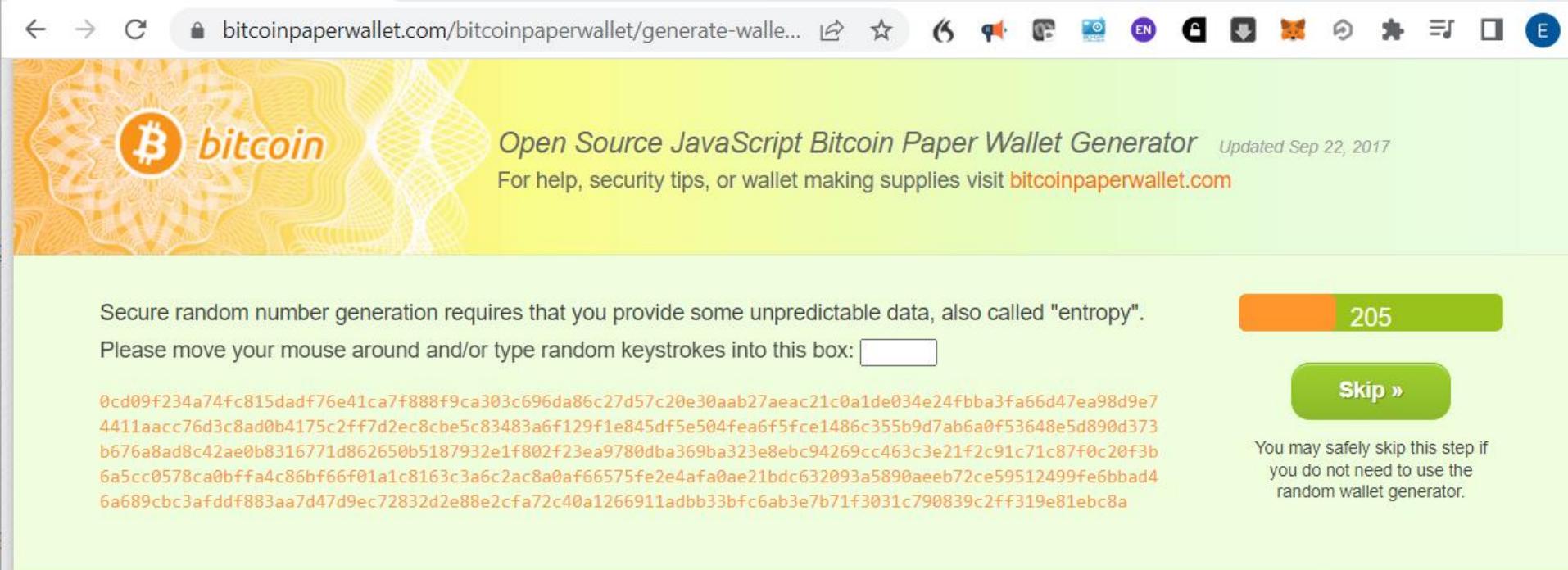

Share 1: 3XxMpaEGgCHkNoLL69NCelWkNA34LBvG3MaYXmvpyu9aWg


Share 2: 3Y2o1pm1a4rdwfnhCtp7so6Dmq1zpVeszTE2ZzWizPHpT2j


Share 3: 3Y8RgccdtoKG4vbbHdxXudBAqovcvEbBaJcn4mULHb7gVza


bitaddress.org

BitcoinPaperWallet.com



Open Source JavaScript Bitcoin Paper Wallet Generator Updated Sep 22, 2017

For help, security tips, or wallet making supplies visit bitcoinpaperwallet.com

Secure random number generation requires that you provide some unpredictable data, also called "entropy".

Please move your mouse around and/or type random keystrokes into this box:

205

Skip »

You may safely skip this step if you do not need to use the random wallet generator.

```
0cd09f234a74fc815dadf76e41ca7f888f9ca303c696da86c27d57c20e30aab27aeac21c0a1de034e24fbba3fa66d47ea98d9e7  
4411aacc76d3c8ad0b4175c2ff7d2ec8cbe5c83483a6f129f1e845df5e504fea6f5fce1486c355b9d7ab6a0f53648e5d890d373  
b676a8ad8c42ae0b8316771d862650b5187932e1f802f23ea9780dba369ba323e8ebc94269cc463c3e21f2c91c71c87f0c20f3b  
6a5cc0578ca0bffa4c86bf66f01a1c8163c3a6c2ac8a0af66575fe2e4afa0ae21bdc632093a5890aeeb72ce59512499fe6bbad4  
6a689cbc3afddf883aa7d47d9ec72832d2e88e2cfa72c40a1266911adbb33bfc6ab3e7b71f3031c790839c2ff319e81ebc8a
```

Encrypted Wallets

Your **public** key is: **1M9VcL4HJY9EAiTG18twLMF3kf8f7PhSX4**
Receive bitcoin to your wallet using your PUBLIC key.

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 + Horizontal

WALLET

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](#)

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

One moment please...

Encrypting your wallet. This may take up to
several minutes on a slower computer.

Online paper wallet generators

Not secure

- Who is hosting the web page and potentially intercepting your private key?
- Did you go to 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-dec17c07685e1870960903d8f58090475b25af94fe95a734f88408cef4aa194.html>
 - <https://bitcoinpaperwallet.com/bitcoinpaperwallet/generate-wallet.html>
2. Print the paper wallet as a PDF file and save it to your computer.