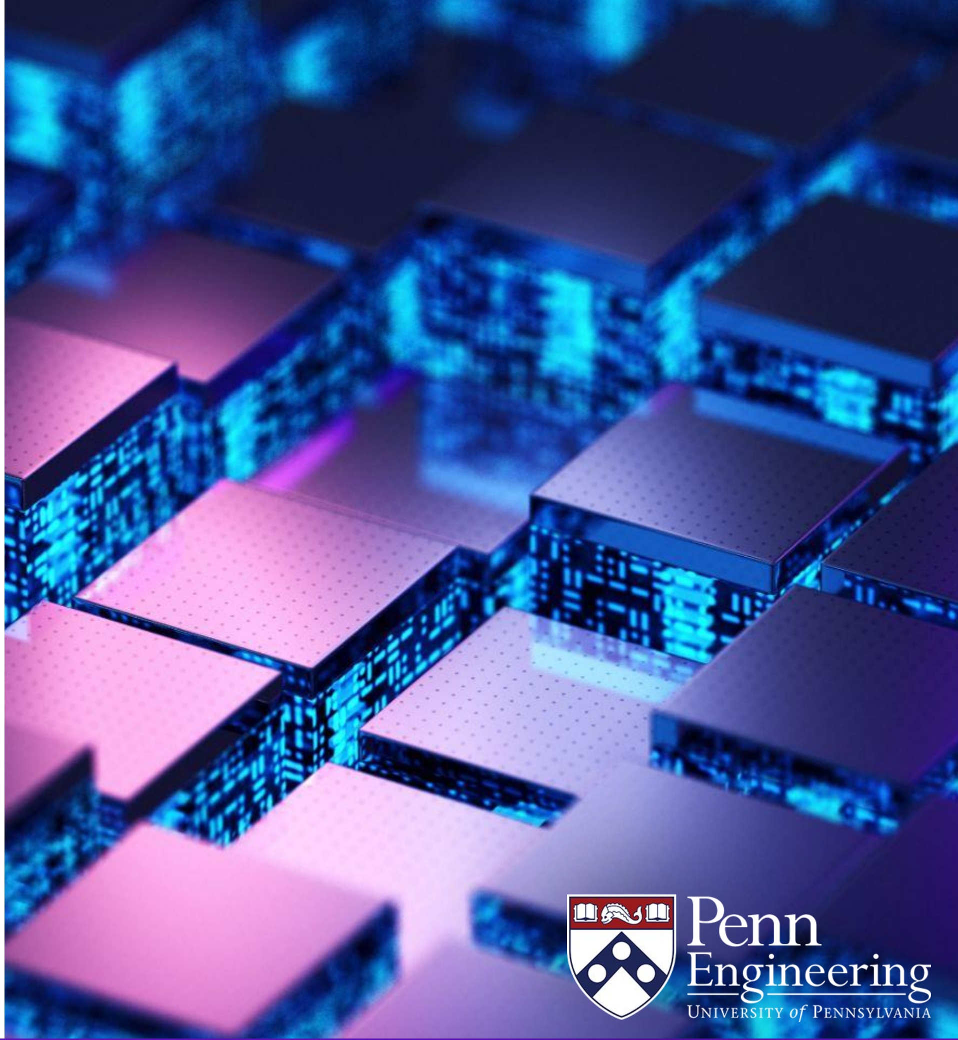
EAS 5830: BLOCKCHAINS

Signatures on the blockchain

Professor Brett Hemenway Falk



Bitcoin is Not Using Encryption

- Bitcoin
  - Transactions are unencrypted
  - Messages between peers are unencrypted
  - Blockchain is unencrypted
  - Transactions are *signed* by their originator

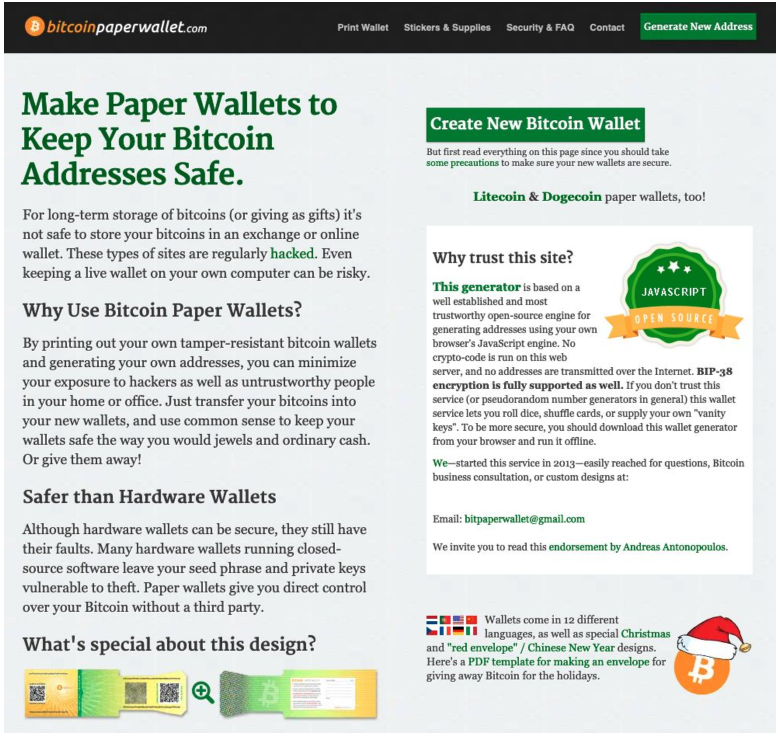
Signatures on the Blockchain

- Accounts are indexed by public keys (verification keys)
- Withdrawals require a signature from the associated signing key
- No attempt to link accounts to real-world identities
- Man-in-the-Middle attacks are possible
  - How do you know you're sending to the right address?
- Signatures guarantee the source of the transaction
- Transactions themselves are public
  - (but pseudonymous)

Creating Accounts

- Accounts on Bitcoin and Ethereum are key pairs for the standard Elliptic Curve Digital Signature Algorithm (ECDSA)
- This means you can create accounts using standard cryptographic software
  - Here's a tutorial to create an account with OpenSSL
  - Later we'll create accounts using Python

Javascript wallet generators



Make Paper Wallets to Keep Your Bitcoin Addresses Safe.

For long-term storage of bitcoins (or giving as gifts) it's not safe to store your bitcoins in an exchange or online wallet. These types of sites are regularly hacked. Even keeping a live wallet on your own computer can be risky.

Why Use Bitcoin Paper Wallets?

By printing out your own tamper-resistant bitcoin wallets and generating your own addresses, you can minimize your exposure to hackers as well as untrustworthy people in your home or office. Just transfer your bitcoins into your new wallets, and use common sense to keep your wallets safe the way you would jewels and ordinary cash. Or give them away!

Safer than Hardware Wallets

Although hardware wallets can be secure, they still have their faults. Many hardware wallets running closed-source software leave your seed phrase and private keys vulnerable to theft. Paper wallets give you direct control over your Bitcoin without a third party.

What's special about this design?

But first read everything on this page since you should take some precautions to make sure your new wallets are secure.

Litecoin & **Dogecoin** paper wallets, too!

Why trust this site?

This generator is based on a well established and most trustworthy open-source engine for generating addresses using your own browser's JavaScript engine. No crypto-code is run on this web server, and no addresses are transmitted over the Internet. **BIP-38 encryption is fully supported as well.** If you don't trust this service (or pseudorandom number generators in general) this wallet service lets you roll dice, shuffle cards, or supply your own "vanity keys". To be more secure, you should download this wallet generator from your browser and run it offline.

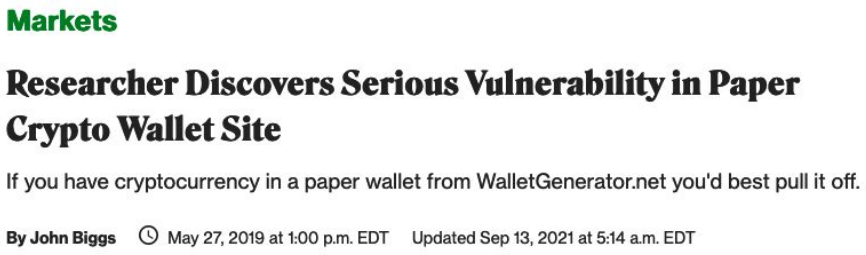
We—started this service in 2013—easily reached for questions, Bitcoin business consultation, or custom designs at:

Email: bitpaperwallet@gmail.com

We invite you to read this endorsement by Andreas Antonopoulos.

Wallets come in 12 different languages, as well as special Christmas and "red envelope" / Chinese New Year designs. Here's a PDF template for making an envelope for giving away Bitcoin for the holidays.

Javascript wallet generators

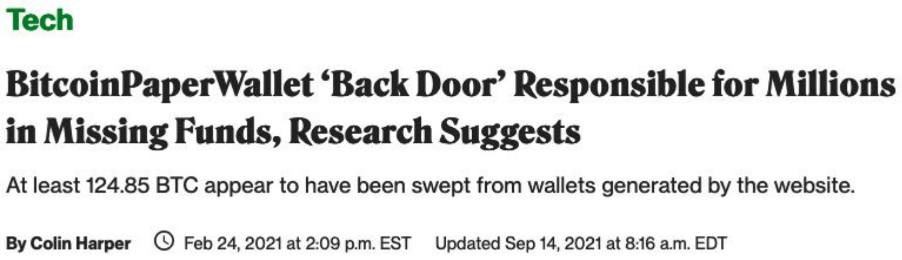


Markets

Researcher Discovers Serious Vulnerability in Paper Crypto Wallet Site

If you have cryptocurrency in a paper wallet from WalletGenerator.net you'd best pull it off.

By John Biggs May 27, 2019 at 1:00 p.m. EDT Updated Sep 13, 2021 at 5:14 a.m. EDT



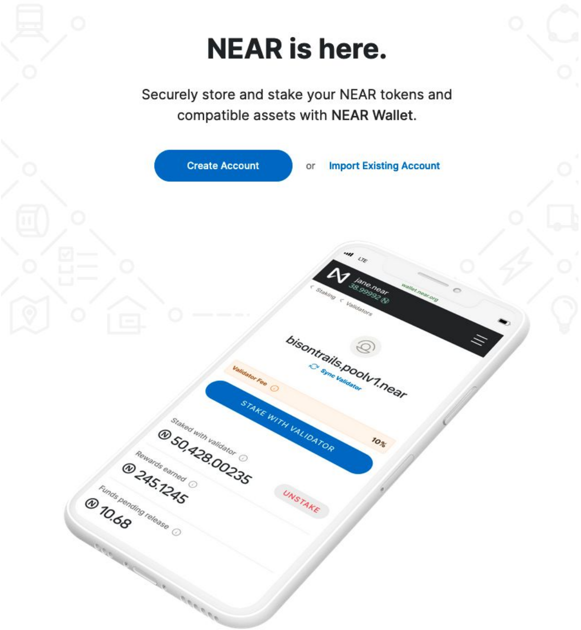
Tech

BitcoinPaperWallet 'Back Door' Responsible for Millions in Missing Funds, Research Suggests

At least 124.85 BTC appear to have been swept from wallets generated by the website.

By Colin Harper Feb 24, 2021 at 2:09 p.m. EST Updated Sep 14, 2021 at 8:16 a.m. EDT

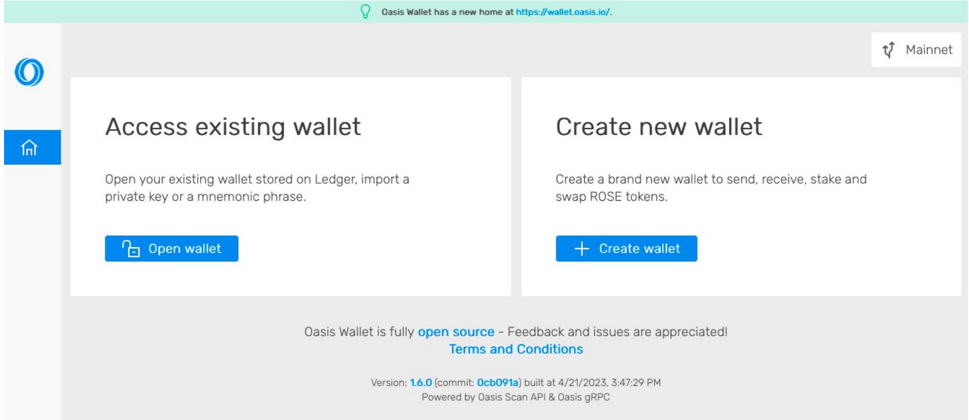
Javascript wallet generators



NEAR is here.

Securely store and stake your NEAR tokens and compatible assets with **NEAR Wallet**.

Create Account or Import Existing Account



Oasis Wallet has a new home at https://wallet.oasis.io/.

Mainnet

Access existing wallet

Open your existing wallet stored on Ledger, import a private key or a mnemonic phrase.

Open wallet

Create new wallet

Create a brand new wallet to send, receive, stake and swap ROSE tokens.

+ Create wallet

Oasis Wallet is fully open source - Feedback and issues are appreciated!
Terms and Conditions

Version: 1.6.0 (commit: 0cb091a) built at 4/21/2023, 3:47:29 PM
Powered by Oasis Scan API & Oasis gRPC

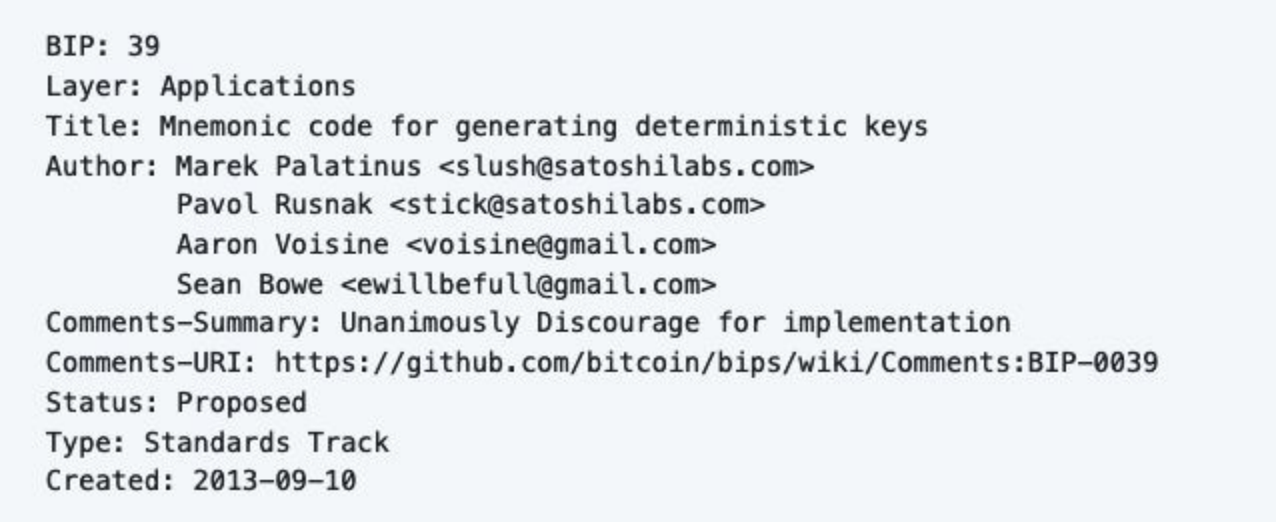
Wallet software

Hardware wallets

Private Keys

- What software generated your private key?
  - Did it use sufficient entropy?
    - The Profanity address generator used too little entropy which led to millions in losses
  - Did it send the private key to someone else?
- Did you back up your private key?

BIP-39 Seed Phrases



```
BIP: 39
Layer: Applications
Title: Mnemonic code for generating deterministic keys
Author: Marek Palatinus <slush@satoshilabs.com>
        Pavol Rusnak <stick@satoshilabs.com>
        Aaron Voisine <voisine@gmail.com>
        Sean Bowe <ewillbefull@gmail.com>
Comments-Summary: Unanimously Discourage for implementation
Comments-URI: https://github.com/bitcoin/bips/wiki/Comments:BIP-0039
Status: Proposed
Type: Standards Track
Created: 2013-09-10
```

Account Abstraction

HOME / ETHEREUM ROADMAP / ACCOUNT ABSTRACTION

Page last updated: June 8, 2023

Account abstraction

Account Abstraction

- Tokens are held by a smart contract wallet
- Users send requests (“intentions”) to the wallet contract
    - Intentions need to be signed to get on the blockchain
        - This can be done by the user themself or a relayer
- Wallet contract can use arbitrary logic to decide whether to process these requests
    - Different signature schemes (post-quantum)
    - Allow / Deny lists
    - Spending limits
    - Multiple Approvers

Penn
Engineering
UNIVERSITY of PENNSYLVANIA