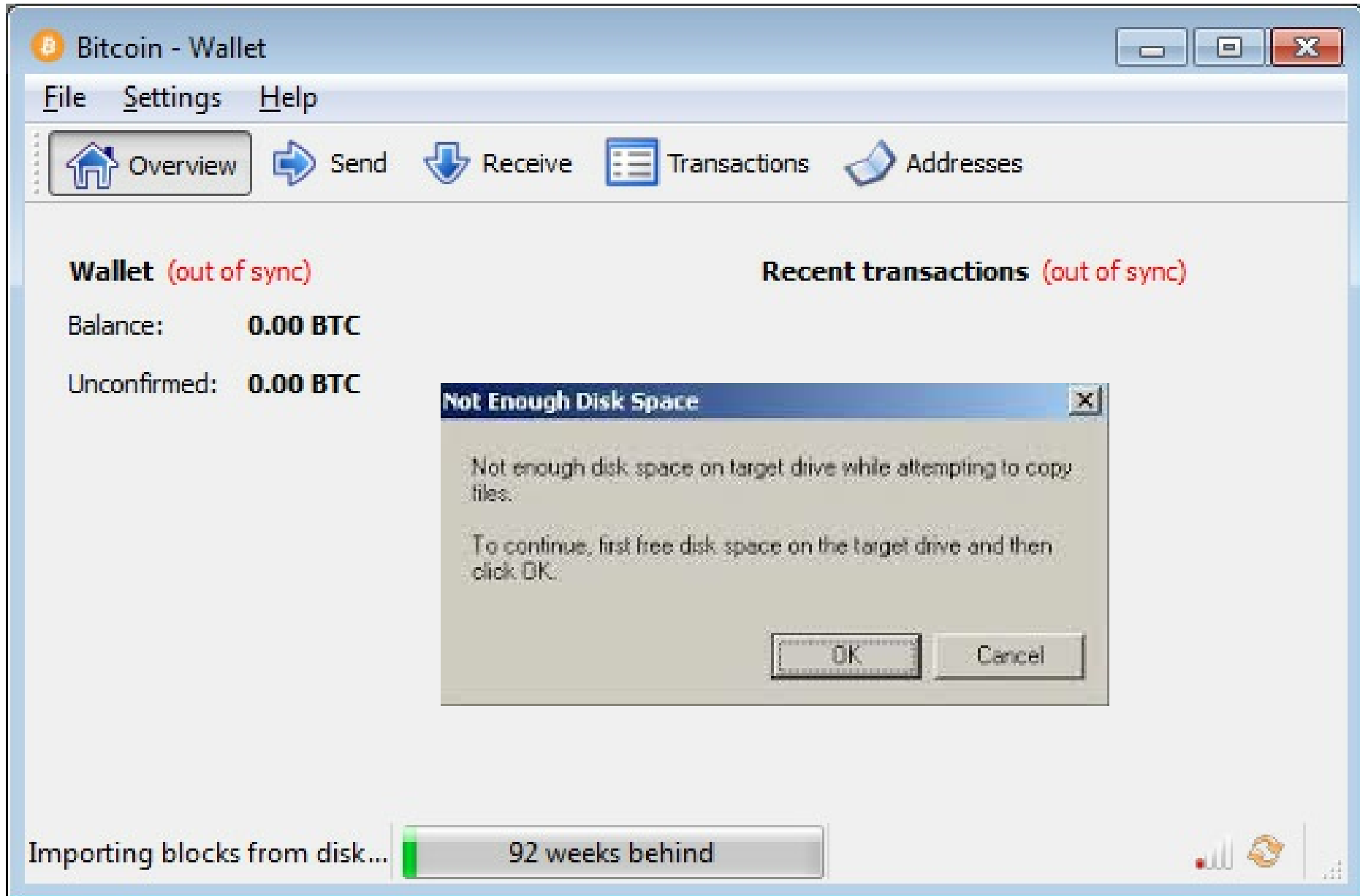
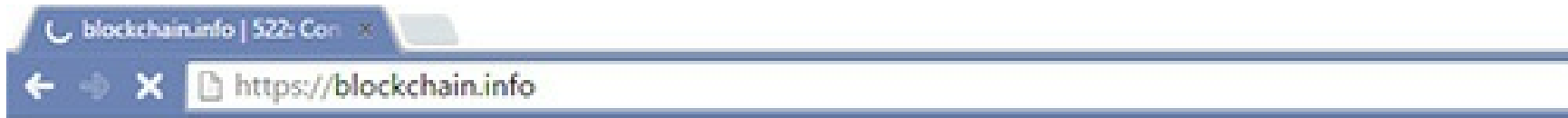


Concept of Bitcoin wallet security

Desktop Bitcoin wallet problems



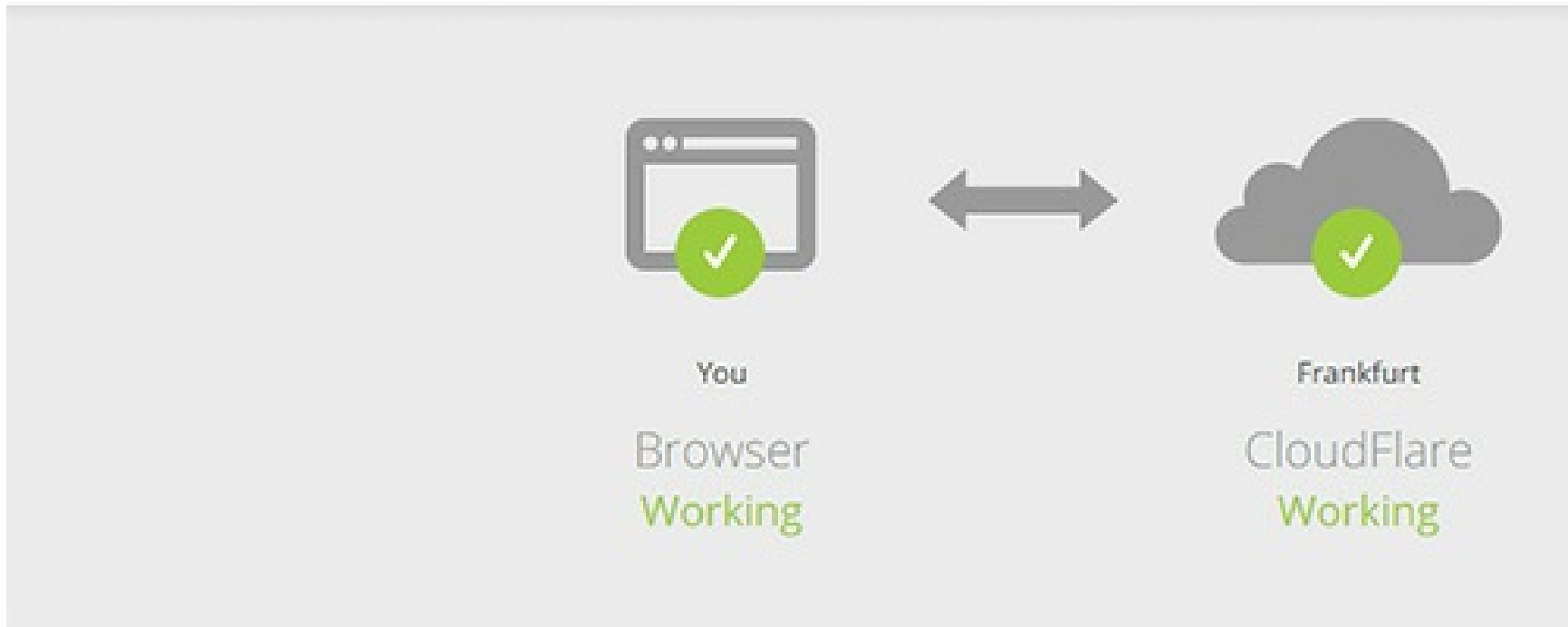
Online Bitcoin Wallets problems



Error 522

Ray ID: 24d4fc2f706726d8 • 2015-11-3

Connection timed out



How to solve these problems for end user wallets?

Use Blockchain API service provider

(no disk space required, no wait for synchronization)

Use any available Blockchain API service

(independence from service provider)

Store wallet reserve copy in Blockchain

(independence from physical device)

Store wallet reserve copy in Blockchain

Email (login)

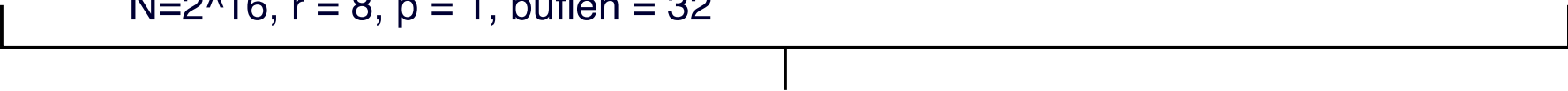
Password

Blockchain password

Use Key derivation function to prevent bruteforce attack

Script (Email + password + blockchain password)

$N=2^{16}$, $r = 8$, $p = 1$, $buflen = 32$



Encryption password

Use AES(Rijndael) to crypt private key

Location in Blockchain

Get ECDSA public key from our encryption password

Send transaction to this public key (bitcoin address)
and store encrypted data in OP_RETURN output

How to get reserve copy from Blockchain

Wallet software calculate blockchain location address using Email Password and Blockchain password

Use any available blockchain service provider to download transactions related to this bitcoin address

Decrypt private key

Any questions?

admin@bitaps.com

Karpov Aleksei
Boyarov Maxim

