



# **Съхранение и използване на криптовалути, портфейли, сигурност**

Владислав Драмалиев  
Директор, Фондация „Битхоуп“  
Мениджър маркетинг и общество, æternity



# Съдържание

1. Предходна лекция
2. Какво е портфейл?
  1. Bitcoin Core
  2. [H]D портфейли
  3. Какво е “seed”?
3. Видове портфейли
  - I. Десктоп
  - II. Онлайн
  - III. Мобилни
  - IV. Хардуерни
  - V. „Хартиени“
4. Управление на пароли
5. 2FA
  - I. Защо да го използваме?
  - II. Видове 2FA



# Предходна лекция

- Кой е първият консенсусен механизъм?
- Какъв алгоритъм за копаене използва æternity?
- Основни две причини за въвеждането на PoS?
- Какво е PoB?
- Какво е „политическа“ централизация в случая на блокчейн проект?
- Колко видове централизация има според Балажи Сринивасан?



# Предходна лекция

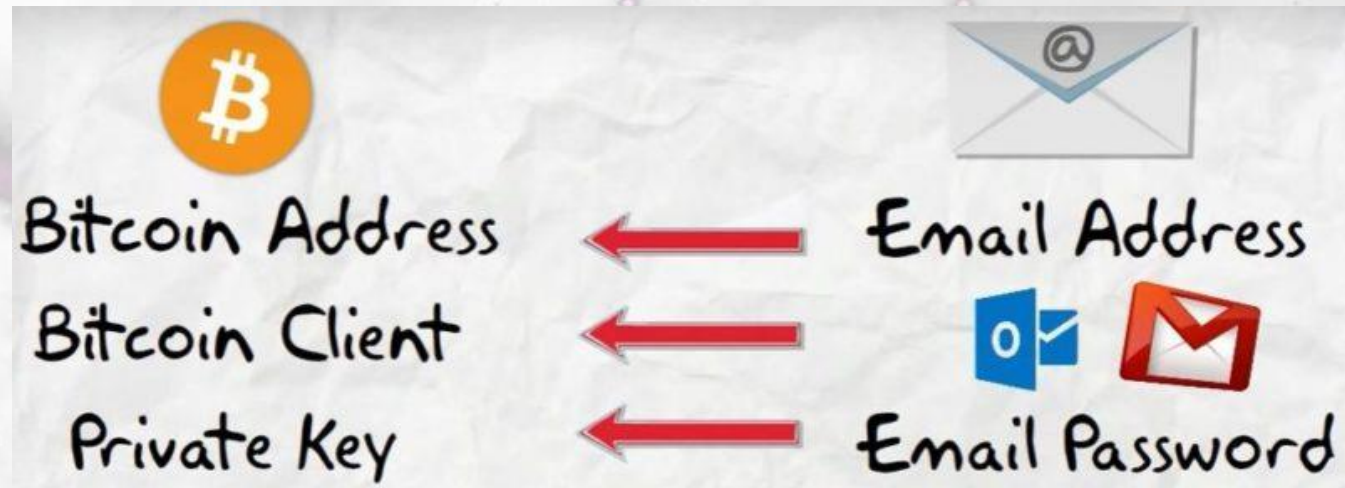
- Кой е първият консенсусен механизъм?
  - Proof-of-Work
- Какъв алгоритъм за копаене използва æternity?
  - Cuckoo Cycle
- Основни две причини за въвеждането на PoS?
  - Избягване на централизация на копаенето + намаляване на електропотреблението
- Какво е PoB?
  - Proof-of-Burn | Изпращане на койни към адрес от който не може да се „харчи“.
- Какво е „политическа“ централизация в случая на блокчейн проект?
  - Само един екип работещ върху разработката на софтуера
- Колко видове централизация има според Балажи Сринивасан?
  - 6. Mining, Client, Developers, Exchanges, Nodes, Ownership.





# Какво е криптопортфейл?

- Мястото, където съхранявате вашите публичен/частен ключ двойки
- Съдържа частните ви ключове



- [Биткойн] адрес (публичен) + частен ключ (таен) = [Биткойн] портфейл

# Какво е криптопортфейл?

- Фундаментален интерфейс, с който комуникирате с блокчейна
- Позволява ви да бъдете „банка“
- Позволява ви да разполагате с валутата си както прецените

**Как/къде се съхранява информацията?**



# Какво е криптопортфейл?

Bitcoin Core

## Bitcoin Core -> wallet.dat

- При инсталация – започва да сваля блокчейна
- Съхранява двойките ключове (ключ/“катионар”) във файл

*C:\Users\YourUserName\AppData\Roaming\Bitcoin*

## Какво съдържа?

Двойки ключове	Акаунти
От/до трансакции	Номер на версията
Настройки на потребителя	<b><u>„Басейн“ от ключове – 100 генерирани</u></b>
Адрес по подразбиране	Информация за блокчейна
Резервни адреси	



# Какво е криптопортфейл?

Bitcoin Core

## Bitcoin Core -> Проблем?

- В случай на прилагането на добри практики
- Прекалено много адреси > 100
- Не е ОК -> един адрес
- Загуба на релевантен бекъп
- **<вече поддържа HD>**

Благодарим ви за дефлацията!





# Какво е криптопортфейл?

[H]D портфейли

## **HD -> Hierarchical Deterministic**

Техническите аспекти на HD портфейлите са представени в [BIP32](#)

Някои са само Deterministic

- Генерират адреси на базата на число, започващо с 1

Hierarchical Deterministic

- По-интересни
- По-широко използвани



# Какво е криптопортфейл?

HD портфейли

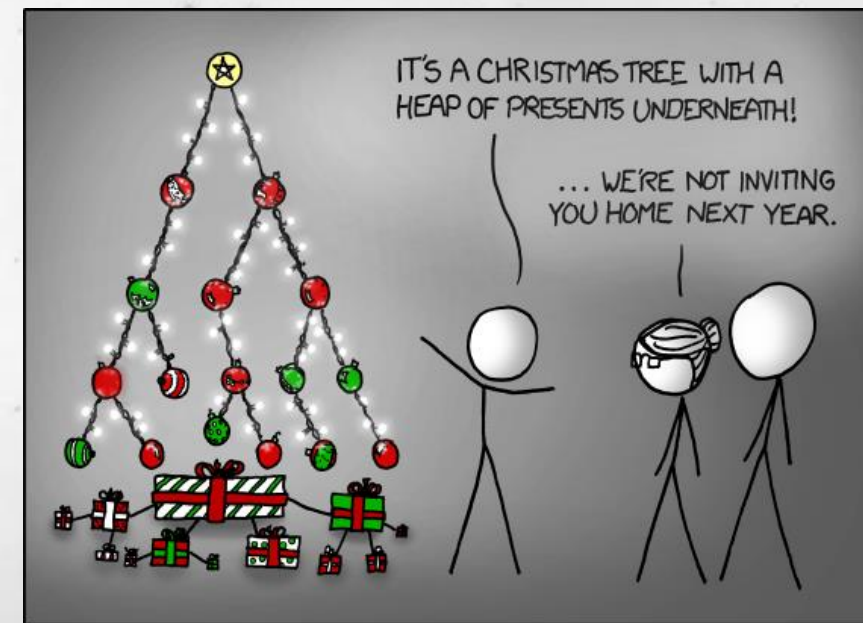
**HD -> Hierarchical Deterministic**

## Hierarchical

- Отново структура, приличаща на дърво
- Позволява разделяне на частни/публични ключове

## Deterministic

- Главният ключ (master key) произвежда същото „дърво“



# Какво е криптопортфейл?

HD портфейли

**HD -> Hierarchical Deterministic**

Отново два вида ключове – **Публичен и Частен**

Главен Публичен ключ (Master Public Key)

- Може да се използва за генериране на безкрайно много „адреси“
- Няма достъп до частните ключове
- Много полезен за борсите

Главен Частен ключ (Master Private Key)

- Генерира всички частни ключове
- Може никога да не „докосва“ интернет



# Какво е криптопортфейл?

HD портфейли

**HD -> Hierarchical Deterministic**

Mnemonic phrase / Mnemonic recovery phrase / Mnemonic seed = Seed

witch collapse practice feed shame open despair creek road again ice least

Произволно подреждане на думи от списък с 2048 ([BIP39 стандарт](#))

$2048 * 2048 * 2048 * 2048 * 2048 * 2048 * 2048 * 2048 * 2048 * 2048 * 2048 * 2048$

(2 на 132 степен)





# Какво е криптопортфейл?

HD портфейли

**HD -> Hierarchical Deterministic**

**Три изисквания към списъка с думи:**

- 1) Умен избор на думи – първите 4 букви гарантират идентификация на думата
- 2) Да не включва подобни думи – woman/women, build/built и т.н.
- 3) Подреден списък – по лесно използване

[Списък с думи](#)





# Какво е криптопортфейл?

HD портфейли

**HD -> Hierarchical Deterministic**

Имитация на процеса по произволно избиране на думи – [Diceware](#)

6 думи – 30 хвърляния на зара

1 6 6 6 5  
1 5 6 5 3  
5 6 3 2 2  
3 5 6 1 6  
6 5 2 2 4  
6 4 3 2 6

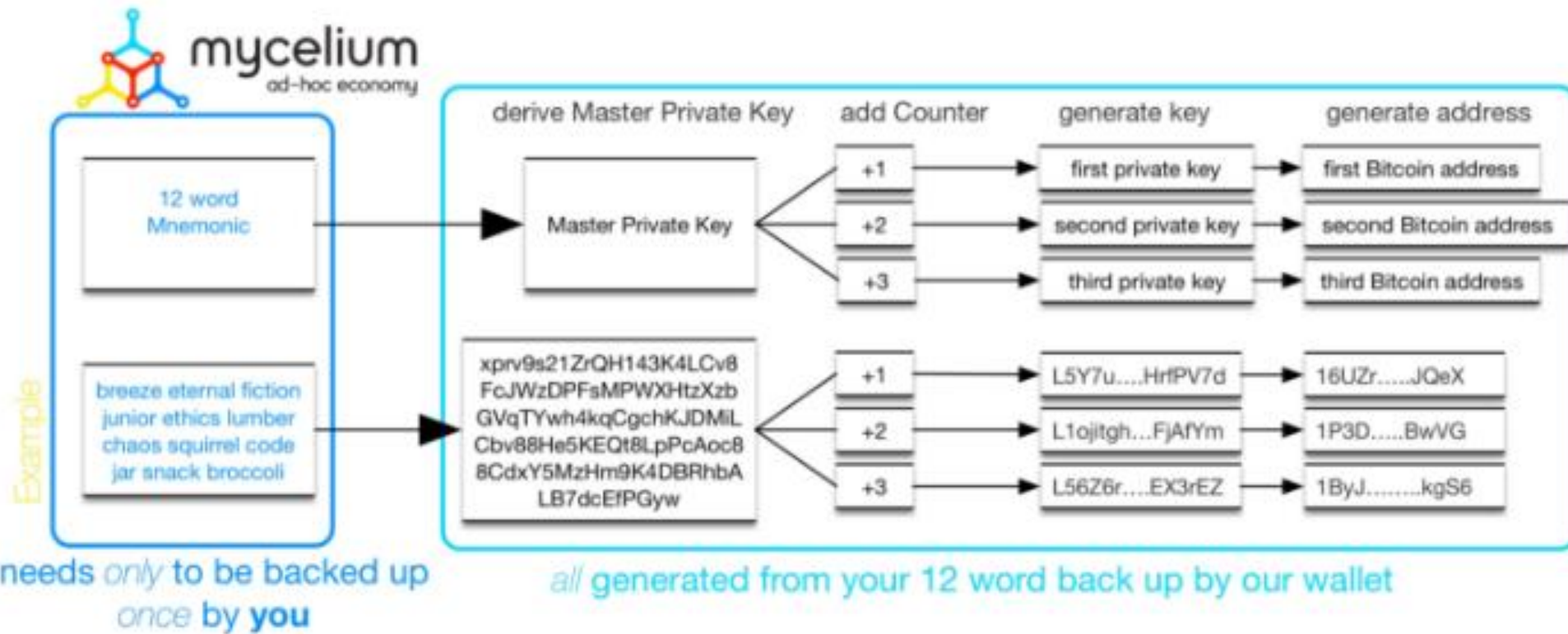
23111 dicta	23241 dock	23411 draco	23541 dud
23112 did	23242 docket	23412 draft	23542 due
23113 dido	23243 dod	23413 drag	23543 duel
23114 die	23244 dodd	23414 drain	23544 duet
23115 died	23245 dodge	23415 drake	23545 duff
23116 diego	23246 dodo	23416 dram	23546 duffy
23121 diem	23251 doe	23421 drama	23551 dug
23122 diesel	23252 doff	23422 drank	23552 dугan
23123 diet	23253 dog	23423 drape	23553 duke
23124 diety	23254 doge	23424 draw	23554 dull
23125 dietz	23255 dogma	23425 drawl	23555 dully
23126 dig	23256 dolan	23426 drawn	23556 dulse
23131 digit	23261 dolce	23431 dread	23561 duly
23132 dilate	23262 dole	23432 dream	23562 duma
23133 dill	23263 doll	23433 dreamy	23563 dumb
23134 dim	23264 dolly	23434 dreg	23564 dummy
23135 dime	23265 dolt	23435 dress	23565 dump
23136 din	23266 dome	23436 dressy	23566 dumpy
23141 dinah	23311 don	23441 drew	23611 dun
23142 dine	23312 don't	23442 drib	23612 dunce
23143 ding	23313 done	23443 dried	23613 dune
23144 dingo	23314 doneck	23444 drier	23614 dung
23145 dingy	23315 donna	23445 drift	23615 dunham
23146 dint	23316 donor	23446 drill	23616 dunk
23151 diode	23321 doom	23451 drink	23621 dunlop
23152 dip	23322 door	23452 drip	23622 dunn
23153 dirac	23323 dope	23453 drive	23623 dupe
23154 dire	23324 dora	23454 droll	23624 durer
23155 dirge	23325 doria	23455 drone	23625 dusk
23156 dirt	23326 doric	23456 drool	23626 dusky
23161 dirty	23331 doris	23461 droop	23631 dust
23162 dis	23332 dose	23462 drop	23632 dusty
23163 disc	23333 dot	23463 dross	23633 dutch
23164 dish	23334 dote	23464 drove	23634 duty
23165 disk	23335 double	23465 drown	23635 dv
23166 disney	23336 doubt	23466 drub	23636 dw
23211 ditch	23341 douce	23511 drug	23641 dwarf
23212 ditto	23342 Doug	23512 druid	23642 dwell
23213 ditty	23343 dough	23513 drum	23643 dwelt
23214 diva	23344 dour	23514 drunk	23644 dwight
23215 divan	23345 douse	23515 drury	23645 dwyer
23216 dive	23346 dove	23516 dry	23646 dx
23221 dixie	23351 dow	23521 dryad	23651 dy
23222 dixon	23352 dowel	23522 ds	23652 dyad
23223 dizzy	23353 down	23523 dt	23653 dye
23224 dj	23354 downs	23524 du	23654 dyer
23225 dk	23355 dowry	23525 dual	23655 dying
23226 dl	23356 doyle	23526 duane	23656 dyke
23231 dm	23361 doze	23531 dub	23661 dylan
23232 dn	23362 dozen	23532 dubhe	23662 dyne
23233 dna	23363 dp	23533 dublin	23663 dz
23234 do	23364 dq	23534 ducat	23664 e



# Какво е криптопортфейл?

HD портфейли

**HD -> Hierarchical Deterministic**



# Видове портфейли

**Съществуват няколко вида портфейли:**

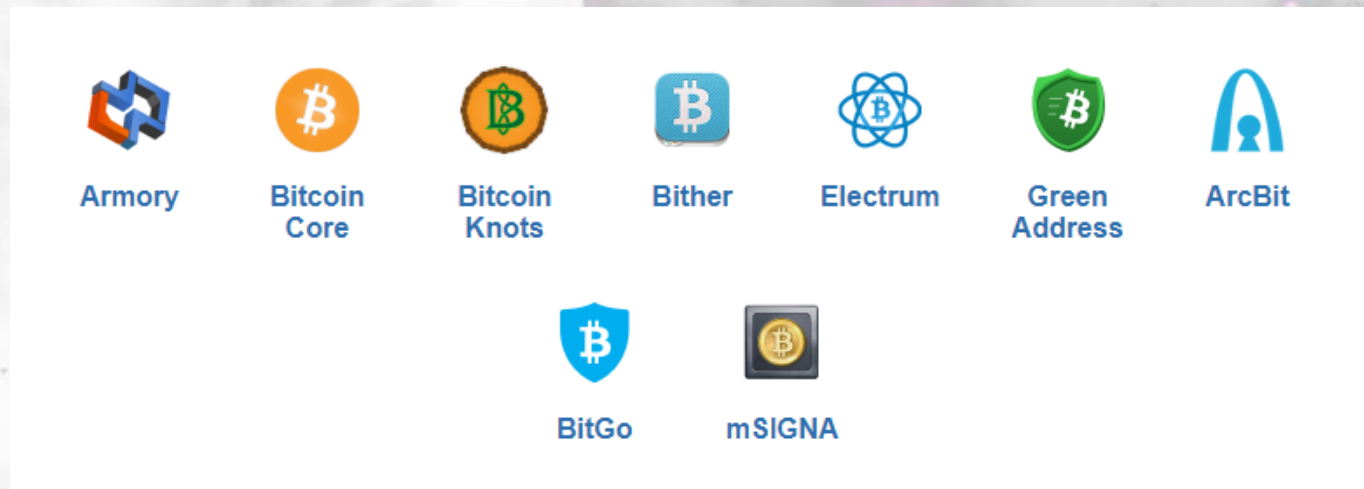
1. Десктоп
2. Онлайн
3. Мобилни
4. Хардуерни
5. „Хартиени“



# Видове портфейли

## Десктоп


- Инсталират се на компютър
- Могат да се използват само на компютъра, на който са инсталирани\*
- Добро ниво на защита
- Защиават частните ви ключове във файл на компютъра ви
- Обикновено този файл е криптиран с парола
- Key-loggers!!!
- Screen-viewers!!!







# Видове портфейли


Десктоп – Bitcoin Core


 **Windows**

[Install](#) [Source code](#)


 **Control over your money** ?


 **Full validation** ?

 **Complete transparency** ?

 **Vulnerable environment** ?

This wallet can be loaded on computers which are vulnerable to malware. Securing your computer, using a strong passphrase, moving most of your funds to cold storage, or enabling two-factor authentication can make it harder to steal your bitcoins.

 **Improved privacy** ?

 **Full control over fees** ?

Bitcoin Core - Wallet

[Overview](#) [Send](#) [Receive](#)

**Wallet**  
Available: **40.20 mBTC**  
Pending: **0.00 mBTC**  


---

Total: **40.20 mBTC**





# Видове портфейли

Десктоп – Electrum


 **Windows**


[Visit website](#) [Source code](#)


 **Control over your money** ?

 **Simplified validation** ?

This wallet uses SPV and random servers from a list. This means little trust in third parties is required when verifying payments. However, it is not as secure as a full node like [Bitcoin Core](#).

 **Basic transparency** ?


 **Two-factor authentication** ?

 **Basic privacy** ?

**Prevents spying on your payments**  
This wallet makes it harder to spy on your balance and payments by rotating addresses. You should still take care to use a new Bitcoin address each time you request payment.




**Discloses information to a third party**  
This wallet uses central servers which are able to associate your payments together and log your IP address.

**Tor can be used**  
This wallet lets you setup and use [Tor](#) as a proxy to prevent attackers or Internet service providers from associating your payments with your IP address.


 **Full control over fees** ?

Electrum 1.9.6

History Send Receive Contacts Console


Date	Description
 2014-07-09 13:25	Gift
 2014-07-09 13:09	Donation
 2014-07-09 11:57	Received payment

Balance: 0.0432 BTC





# Видове портфейли

Десктоп – GreenAddress


 **Windows**

[Install](#) [Source code](#)


 **Shared control over your money ?**


 **Centralized validation ?**


This wallet relies on a centralized service by default. This means a third party must be trusted to not hide or simulate payments.


 **Remote app ?**

This wallet is loaded from a remote location. This means that whenever you use your wallet, you need to trust the developers not to steal or lose your bitcoins in an incident on their site. Using a browser extension or mobile app, if available, can reduce that risk.

 **Two-factor authentication ?**

 **Basic privacy ?**

 **Full control over fees ?**

 **GreenAddress.it**

**Balance**

**Transactions**


**Send Money**


**Receive Money**

**Address Book**

**Settings**

**Logout**

 41.90 mBTC


 26.15 USD

FAQ | Support

Last login: 2014-07-09 19:07:00 from  
162.222.147.245 (country: CA)  
Copyright © GreenAddress.it 2014

**WARNING:** You

Last 10 items

 Date

09/07/2014

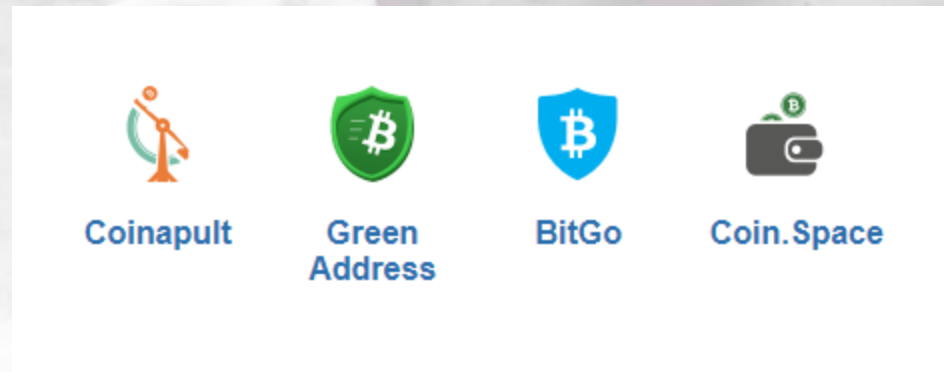
09/07/2014



# Видове портфейли

Онлайн

- Повечето не ви предоставят достъп до частните ви ключове
- Не сте си сами „банка“
- Всички борси са вид онлайн портфейл – няма частни ключове за потребителите



# Видове портфейли


Онлайн – Blockchain.info

## Verify Recovery Phrase

### Security Tip

Do not store your Recovery Phrase on your computer or online. It is very important to keep your Recovery Phrase offline in a safe and private place. Anyone with access to your Recovery Phrase has access to your funds.

We have created a printable Recovery Sheet to help you conveniently keep your Recovery Phrase safe. Print the blank Recovery Sheet and then move onto the next step to fill it in.

 [Print Recovery Sheet](#)

Close

Next Step

## Recover Funds

Step 1 of 2: Enter 12 word passphrase

Recover bitcoins from your lost wallet



**You should always pair or login if you have access to your Wallet ID and password. Recovering your funds will create a new Wallet ID.**

### Your Recovery Passphrase

Enter your 12 recovery words with spaces to recover your funds & transactions


Go Back

Continue




# Видове портфейли


Онлайн – BitGo


 Web


[Visit website](#)


 Shared control over your money ?


This wallet requires every transaction to be authorized both by you and this third party. Under normal circumstances, you can regain full control over your bitcoins using your initial backup or pre-signed transactions sent by email.


 Centralized validation ?

 Remote app ?

 Two-factor authentication ?

 Basic privacy ?

 Dynamic fee suggestions ?

 BitGo ben@bitgo.com

**Secure Wallet** 13.7089 BTC  
\$ 3,214.19 USD

2My3hs7kU6ZNNWfayXx9cFehnNL4n4gFGg7

[Send](#) [Receive](#)

Send To

Mikes Wallet 2N5en6cQ...j7v42S4U x

Amount

This transaction exceeds your spending limit.

BTC 3.14 \$ 736.55 USD

Internal Memo


Enter a memo (optional)

[Next](#)




# Видове портфейли


Онлайн – BitGo


 Web


[Visit website](#)


 Shared control over your money ?


This wallet requires every transaction to be authorized both by you and this third party. Under normal circumstances, you can regain full control over your bitcoins using your initial backup or pre-signed transactions sent by email.


 Centralized validation ?

 Remote app ?

 Two-factor authentication ?

 Basic privacy ?

 Dynamic fee suggestions ?

 BitGo ben@bitgo.com

**Secure Wallet** 13.7089 BTC  
\$ 3,214.19 USD

2My3hs7kU6ZNNWtAyXx9cFehnNL4n4gFGg7

[Send](#) [Receive](#)

Send To

Mikes Wallet 2N5en6cQ...j7v42S4U x

Amount

This transaction exceeds your spending limit.

BTC 3.14 \$ 736.55 USD

Internal Memo

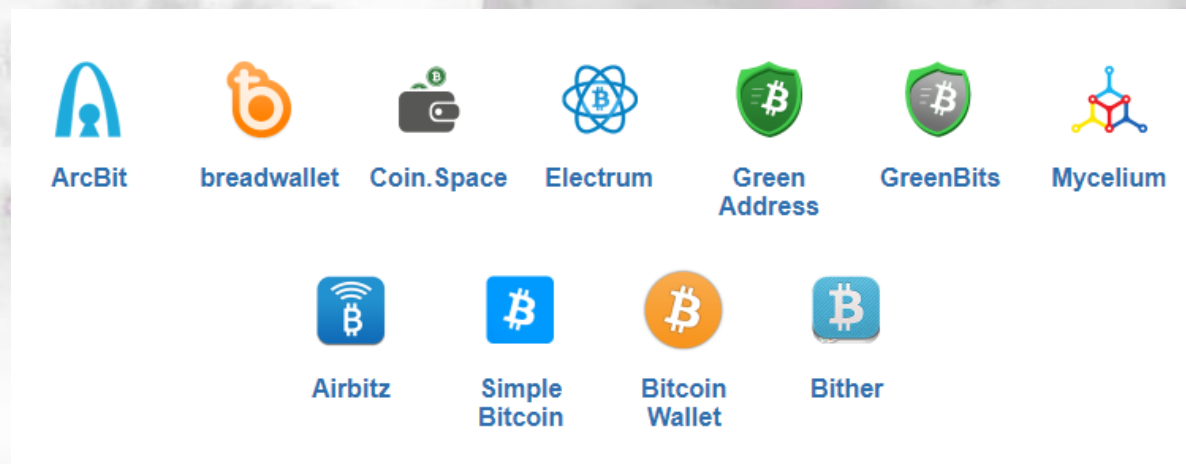
Enter a memo (optional)

[Next](#)

# Видове портфейли


## Мобилни

- Използват се на мобилни устройства
- Обикновено са по-лесни за използване (по-малко функции)
- HD




# Видове портфейли


Мобилни - Mycelium

 **Android**


**Install**

**Source code**


 **Control over your money** ?


 **Centralized validation** ?

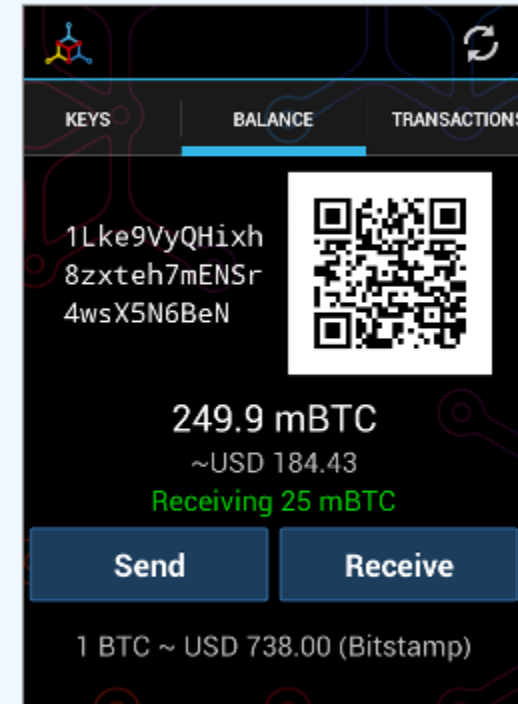
This wallet relies on a centralized service by default. This means a third party must be trusted to not hide or simulate payments.

 **Basic transparency** ?

 **Secure environment** ?

 **Basic privacy** ?

 **Dynamic fee suggestions** ?

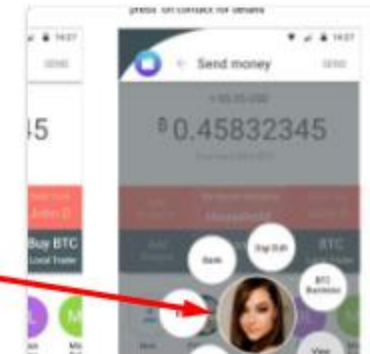
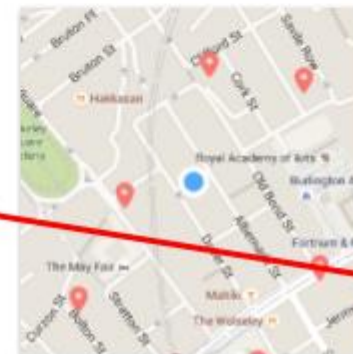
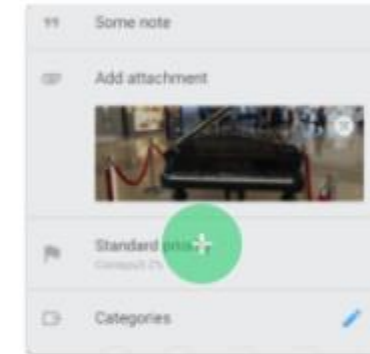
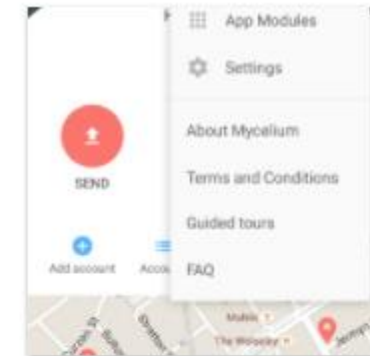


# Видове портфейли

Мобилни - Mycelium

## Top 7 New Tools Coming Soon

- 1] Fiat accounts: fully-fledged, blockchain based.
- 2] Inexpensive remittance: most popular corridors.
- 3] Debit cards. Wallet - linked and in-wallet-issued.
- 4] Personal finance: convenient handling of bills and invoices.
- 5] Investments: efficient portfolios and hedging.
- 6] Escrow-protected business transactions and bets.
- 7] Crypto assets creation and exchange.



Sasha Gray :D



# Видове портфейли

## Мобилни - ?!?!

## Sasha Grey

From Wikipedia, the free encyclopedia

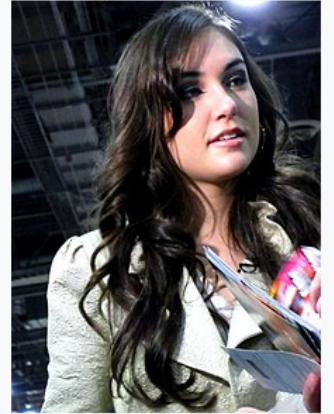
**Sasha Grey** (born **Marina Ann Hantzis**;<sup>[3]</sup> March 14, 1988) is an American actress, model, and musician,<sup>[4][5]</sup> and **former pornographic actress**.<sup>[6][7]</sup> She first made her name in mainstream media after appearing on several popular television programs and in pop culture magazines, examining her willingness to enter the world of **hardcore porn** at a young age.<sup>[8][9]</sup> She has also been featured in movies, television shows, music videos and **advertising campaigns**.<sup>[10][11]</sup> She won numerous awards for her work in pornography between 2007 and 2010, including the **Female Performer of the Year** at the **2008 AVN Awards**.

After her feature film debut as the lead in Steven Soderbergh's *The Girlfriend Experience* (2009), Grey shifted her focus to mainstream acting.<sup>[7]</sup> She starred in the Canadian black comedy horror film *Smash Cut* (2009)<sup>[12]</sup> and played a fictionalized version of herself in **the seventh season** of the HBO comedy-drama series *Entourage*. She has also appeared in independent films such as *I Melt with You* and *Open Windows*. She is a former member of aTelecine, an industrial music band.<sup>[5][13][14]</sup>

### Contents [hide]

- Background
- Career
  - Appearances
  - Advocacy
  - Modeling
  - Acting
  - Music
  - Books
- Personal life
- Controversies
- Awards
  - Other awards
- Filmography
  - Film
  - Television
  - Music videos
  - Web
  - Video games
- Bibliography
- See also
- References
- External links

Sasha Grey




Grey in 2010

<b>Born</b>	Marina Ann Hantzis March 14, 1988 (age 29) <span>North Highlands, California, U.S.</span>
<b>Other names</b>	Anna Karina, Sascha Grey, Sasha Gray
<b>Height</b>	5 <span> </span> ft 6 <span> </span> in (1.68 <span> </span> m) <sup>[1]</sup>
<b>Weight</b>	110 <span> </span> lb (50 <span> </span> kg) <sup>[1]</sup>
<b>Website</b>	<span>www.SashaGrey.com</span> <span><span></span></span>




# Видове портфейли


Мобилни - Electrum

 Android


[Install](#)

[Source code](#)

 **Control over your money** ?


 **Simplified validation** ?

This wallet uses SPV and random servers from a list. This means little trust in third parties is required when verifying payments. However, it is not as secure as a full node like [Bitcoin Core](#).

 **Basic transparency** ?

 **Secure environment** ?


 **Basic privacy** ?

 **Full control over fees** ?




# Видове портфейли


Мобилни – Bitcoin Wallet


 **Android**

**Install**


**Source code**

 **Control over your money** ?

 Simplified validation ?

 Basic transparency ?

 Secure environment ?

 Basic privacy ?

 **Full control over fees** ?

**Bitcoin**

mBTC **477.06**

≈ USD 112.44



● 21 Apr Donation for Bitcoi... +6.26

● 19:29, 17 April  
Donation for Bitcoin Wallet +13.09

● 17 Apr Donation for Bitcoi... +1.00

● 15 Apr 13tT vECF HS7D A... +0.97

● 14 Apr 1Bq6 P6LV 7L1K m... -1.00

● 12 Apr Donation for Bitcoi... +0.50

◀ REQUEST COINS

SEND COINS ▶



# Видове портфейли





Хардуерни

Горещи Портфейли (Hot Wallets)	Хардуерни Портфейли
Добро решение за малки суми	Най-лесният начин за съхранение
Лесно получаване/изпращане	Поддържат няколко валути
Някои поддържат много валути	ОК, дори на заразени компютри
Генерират двойките ключове онлайн	Двойката ключове - офлайн
Не са 100% сигурни	Подписване на трансакции - офлайн
Неподходящи за големи суми	Струват пари



# Видове портфейли

Хардуерни

	Wallet	Screen	Released	Price
	Ledger Nano S	✓	2016	58€
	TREZOR	✓	2013	\$99
	KeepKey	✓	2015	\$99
	Ledger HW.1	✗	2013	\$17



# Видове портфейли

Хардуерни – Ledger Nano S

Поддържани валути и услуги



BITCOIN



ETHEREUM



LITECOIN



FIDO U2F



DOGECOIN



ZCASH



DASH



STRATIS



RIPPLE



HELLO



BITCOIN CASH



KOMODO



ETHEREUM CLASSIC



POSW



ARK





# Видове портфейли

Хардуерни – Ledger Nano S

## Интеграции



Ledger Wallet Bitcoin

[Learn more](#)



Ledger Wallet Ethereum

[Learn more](#)



Ledger Wallet Ripple

[Learn more](#)



Copay

[Learn more](#)



Electrum

[Learn more](#)



Mycelium

[Learn more](#)



MyEtherWallet

[Learn more](#)



GreenBits

[Learn more](#)



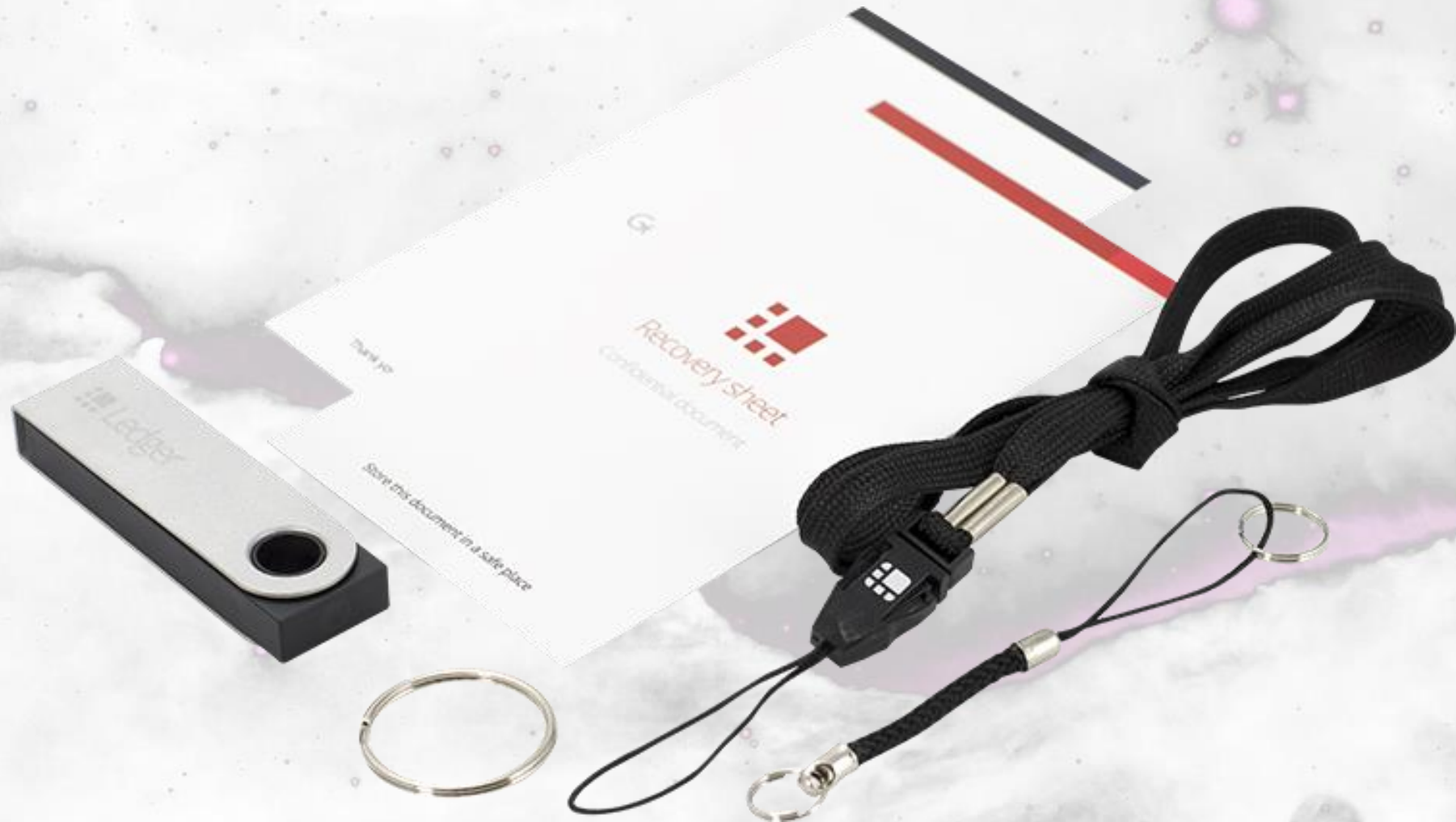
BitGo

[Learn more](#)



# Видове портфейли

Хардуерни – Ledger Nano S



# Видове портфейли

Хардуерни – TREZOR

## Wallet for Bitcoin and others

The most trusted and secure way to store your bitcoins. Protect a variety of alternative digital currencies. Litecoin, DASH and Zcash with a single device.

[Go to Wallet >](#)

## Ethereum integration

Saved under the same seed, secured by the same technology. Use Ethereum conveniently in cooperation with our partners at MyEtherWallet

[Go to MEW >](#)

## Password Manager

Try out the next-generation password management app. Encrypt passwords separately and sync them to your private cloud, hassle-free, with TREZOR.

[Password Manager >](#)

## Secure Admin SSH Access

Protect access to your servers, data or websites administration. SSH login with single or multiple sessions.

[SSH Agent on GitHub >](#)

## 2-Factor Authentication

Safeguard your online accounts and identities. Enable the industry standard FIDO/U2F and use TREZOR as your security token.

[More about U2F >](#)

## Sign & Encrypt with GPG

TREZOR encrypts every document or email you create with GPG.

[GPG via SSH Agent >](#)

## Password-less Login

Securely sign up and login with a click of a button, using TREZOR Connect.

[TREZOR Connect on GitHub >](#)

## Sign & Verify Messages

Easily prove your ownership of messages and documents, or verify others.

[More about Messages >](#)

## Explore Integrations

Connect your TREZOR to third party wallets and services.

[TREZOR Apps >](#)



# Видове портфейли

Хардуерни – TREZOR

Wallet Interfaces for TREZOR by Currency	
Bitcoin	TREZOR Wallet
Litecoin	TREZOR Wallet
DASH	TREZOR Wallet
Zcash	TREZOR Wallet
Bitcoin Cash / Bcash	TREZOR Wallet
Ethereum	MyEtherWallet
Ethereum Classic	MyEtherWallet
ERC-20 Tokens	MyEtherWallet



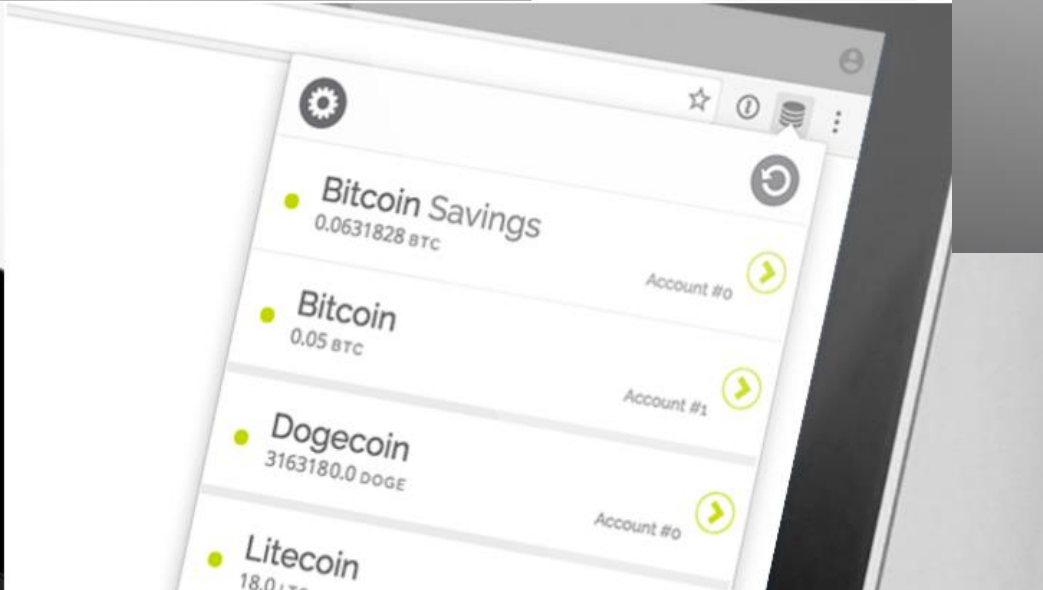
[BitNodes](#)





# Видове портфейли

Хардуерни – KeepKey





# Видове портфейли

Хардуерни – KeepKey

**Does KeepKey support any other digital assets?**

Yes! KeepKey supports Bitcoin, Litecoin, Dogecoin, Namecoin, Testnet, Ethereum, and Dash.

#

## Initialization.

KeepKey generates private key using its hardware-based random number generator, combined with randomness provided by your computer.



RECOVERY SENTENCE

1.power	2.speak	3.east	4.detail	5.pitch
6.debate	7.page	8.solid	9.point	10.you
11.cart	12.cinnamon			

Backup.


Once your private key is generated, you are given the one-time opportunity to write down a backup of your KeepKey in the form of a twelve-word recovery sentence.



# Видове портфейли

Хартиени Портфейли

[English](#) | [Español](#) | [Français](#) | [ελληνικά](#) | [italiano](#) | [Deutsch](#)  
[Česky](#) | [Magyar](#) | [日本語](#) | [简体中文](#) | [Русский](#) | [português](#)

 **bitaddress.org**

Open Source JavaScript Client-Side Bitcoin Wallet Generator

1%

1%

1%

Brain Wallet

1%

1%

Wallet Details

Generating Bitcoin Address...  
MOVE your mouse around to add some extra randomness... 1%  
OR type some random characters into this textbox

70353ff37ca2aac9200b3ae767dbff674a4e19c8d9b70579a10a645a243b7f56514fd3b  
f5a6ff01548ce885bf001413165d76a607a0efbe126ea543d2e285a5c20cee9c12e247b  
ee0ba54a5b4987c5116694901c2674ae5eb6f65a969dd1331c4dcdbdf9f086fe2a63a293  
5da77661b96bbf6c4919105a84b8794793e1e9afc90be3d1a80a08cb5821d2eed24ffe0  
516bea4225f00ddc1a353eb565c1db65c221686971d4856853ae1bdf8c850905809ad5f  
a708c817451b7d2a60ca38467406a55fd92095e94acd2197bc818b74e2b3ae1600f0620  
a1801ad103460347d679a13aa8a8062befd63127a77f0a9cd27dfbf3c3bf38e0520b4f  
fcad8e1f86ef43b

⚠ ✓ ... ☰

Donations: **1NiNja1bUmhSoTXozBRBEtR8LeF9TGbZBN**  
[GitHub Repository](#) ([zip](#))


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

Copyright bitaddress.org. JavaScript copyrights are included in the source. No warranty.




# Видове портфейли

## Хартиени Портфейли

 [Features](#) [Business](#) [Explore](#) [Marketplace](#) [Pricing](#) [This repository](#)  [Sign in](#) or [Sign up](#)

[pointbiz / bitaddress.org](#) [Watch](#) 108 [Star](#) 882 [Fork](#) 884

[Code](#) [Issues](#) 41 [Pull requests](#) 10 [Projects](#) 0 [Insights](#)



### Join GitHub today

GitHub is home to over 20 million developers working together to host and review code, manage projects, and build software together.

[Sign up](#)

[Dismiss](#)

JavaScript Client-Side Bitcoin Wallet Generator <https://www.bitaddress.org>


177 commits










3 branches

15 releases

18 contributors

Branch: **master** [New pull request](#) [Find file](#) [Clone or download](#)

 pointbiz v3.3.0 remove support for IE8 Latest commit 72aefc0 on Dec 24, 2016

 <a href="#">src</a>	v3.3.0 remove support for IE8	10 months ago
 <a href="#">.gitignore</a>	v2.9.9 improve tab usability	2 years ago
 <a href="#">CHANGELOG.txt</a>	v3.3.0 remove support for IE8	10 months ago
 <a href="#">CHANGELOG.txt.asc</a>	v3.3.0 remove support for IE8	10 months ago
 <a href="#">Gruntfile.js</a>	v3.3.0 remove support for IE8	10 months ago
 <a href="#">README.md</a>	v3.3.0 remove support for IE8	10 months ago
 <a href="#">bitaddress.org.html</a>	v3.3.0 remove support for IE8	10 months ago
 <a href="#">bitaddress.org.html.sig</a>	v3.3.0 remove support for IE8	10 months ago
 <a href="#">package.json</a>	v3.3.0 remove support for IE8	10 months ago



# Управление на пароли

## Как съхранявате паролите си?

### Лоши практики:

- Една и съща парола за всичко
- Къса парола
- Само букви, само числа
- „password”, “user”, “12345”

Top 25 most common passwords by year according to SplashData

Rank	2011 <sup>[4]</sup>	2012 <sup>[5]</sup>	2013 <sup>[6]</sup>	2014 <sup>[7]</sup>	2015 <sup>[8]</sup>	2016 <sup>[3]</sup>
1	password	password	123456	123456	123456	123456
2	123456	123456	password	password	password	password
3	12345678	12345678	12345678	12345	12345678	12345
4	qwerty	abc123	qwerty	12345678	qwerty	12345678
5	abc123	qwerty	abc123	qwerty	12345	football
6	monkey	monkey	123456789	123456789	123456789	qwerty
7	1234567	letmein	111111	1234	football	1234567890
8	letmein	dragon	1234567	baseball	1234	1234567
9	trustno1	111111	iloveyou	dragon	1234567	princess
10	dragon	baseball	adobe123 <sup>[a]</sup>	football	baseball	1234
11	baseball	iloveyou	123123	1234567	welcome	login
12	111111	trustno1	admin	monkey	1234567890	welcome
13	iloveyou	1234567	1234567890	letmein	abc123	solo
14	master	sunshine	letmein	abc123	111111	abc123
15	sunshine	master	photoshop <sup>[a]</sup>	111111	1qaz2wsx	admin
16	ashley	123123	1234	mustang	dragon	121212
17	bailey	welcome	monkey	access	master	flower
18	passw0rd	shadow	shadow	shadow	monkey	passw0rd
19	shadow	ashley	sunshine	master	letmein	dragon
20	123123	football	12345	michael	login	sunshine
21	654321	jesus	password1	superman	princess	master
22	superman	michael	princess	696969	qwertyuiop	hottie
23	qazwsx	ninja	azerty	123123	solo	loveme
24	michael	mustang	trustno1	batman	passw0rd	zaq1zaq1
25	Football	password1	000000	trustno1	starwars	password1



# Управление на пароли

Как съхранявате паролите си?

Добри практики:

Използвайте антивирусни програми	„Твърде хубаво, за да е истина“ мейли
Използвайте anti-malware програми	Публични WiFi мрежи (VPN)
Firewall – стандарт	Password Manager! (LastPass)
Обновена на операционната система!	2 Factor Authentication!
Пиратски софтуер...	Pop-up съобщения

# LastPass...!





# Управление на пароли

Provider ↕	Price ↕	Import from browsers ↕	Import from competitors ↕	Two-factor authentication ↕	Export data ↕	Automatic password capture ↕	Automatic password replay ↕	Forms ↕	Multiple form- filling identities ↕	Actionable password strength report ↕	Secure sharing ↕	Digital legacy ↕	Portable edition ↕	Application passwords ↕	Browser menu of logins ↕	Application-level encryption ↕
RoboForm 8	Free or \$19.95	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Dashlane 4	Free or \$39.99	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Encryptr	Free	No	No	No	No	No	No	No	No	No	No	No	No	Yes	No	Yes
Intuitive Password	Free or \$2 (monthly)	No	Yes	Yes	Yes	No	Yes	Yes	No	Yes	Yes	No	Yes	Yes	Yes	Yes
KeePass	Free/Open Source	Yes	Yes	Yes (Plugin)	Yes	Yes	Yes	Yes	Yes	Yes	Optional (Requires add-on server)	No	Yes	Yes	Yes	Yes
KeePassXC	Free/Open Source	Yes	Yes	Yes (Plugin)	Yes	Yes	Yes	Yes	Yes	Yes	No	No	Yes	Yes	Yes	Yes
LastPass 4	Free or \$24.00	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
1Password	\$3-5 (monthly)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Norton Identity Safe	Free	Yes	Yes	No	Yes	Yes	Yes	Yes	Yes	No	No	No	Yes (iOS - US only)	Yes	Yes	Yes



# 2 Factor Authentication

## Видове 2FA

Вид 2FA	Преимущества	Недостатъци
SMS 2FA	<ul style="list-style-type: none"><li>• Код за достъп</li><li>• По-добре от парола/потребител</li></ul>	<ul style="list-style-type: none"><li>• Предоставяне на телефонен номер</li><li>• „Превземане на телефония номер“</li><li>• Обхват!</li></ul>
Authenticator App (TOTP)	<ul style="list-style-type: none"><li>• Код на всяка 1 минута</li><li>• Без връзка с оператора</li></ul>	<ul style="list-style-type: none"><li>• Как се възстановява?</li><li>• Неудобно? (батерия)</li></ul>
Push-based 2FA	<ul style="list-style-type: none"><li>• По-лесно от код – appear/push</li><li>• Показва локация</li></ul>	<ul style="list-style-type: none"><li>• Няма „1 приложение“</li></ul>
FIDO U2F / Security Keys	<ul style="list-style-type: none"><li>• Физическо одобрение</li><li>• „Закача“ се за сайта</li><li>• 1 устройство = много идентичности</li></ul>	<ul style="list-style-type: none"><li>• Поддържа се само от Chrome</li><li>• NFC - Android</li></ul>



*„With Great Power Comes  
Great Responsibility“*

Voltaire [maybe]



# ДИСКУСИЯ/ВЪПРОСИ





vlad@aeternity.com

[www.aeternity.com](http://www.aeternity.com)







SE