

Uvod v Bitcoin in kriptovalute

Jure Pirc
Bitcoin društvo Slovenije
www.bitcoin.si
info@bitcoin.si

Bitcoin denarnice

- Mobilne denarnice
- Polni odjemalci / jedrne denarnice
 - SPV oz lahke denarnice
- Papirnate denarnice (paperwallet)
- Strojne denarnice (hardware wallet)

Mobilne SPV denarnice (simple payment verification)

- Kriptovalute stalno z vami v žepu
- Preprosta varnostna kopija/backup za primer izgube/okvare mobilnika

Take control of your money,
get started with bitcoin.

Get started

Restore from backup



You control your bitcoin.

This app stores your bitcoin with cutting-edge security.



Not even BitPay can access it.

Create bitcoin wallet



Personal Wallet

Please carefully write down this phrase.

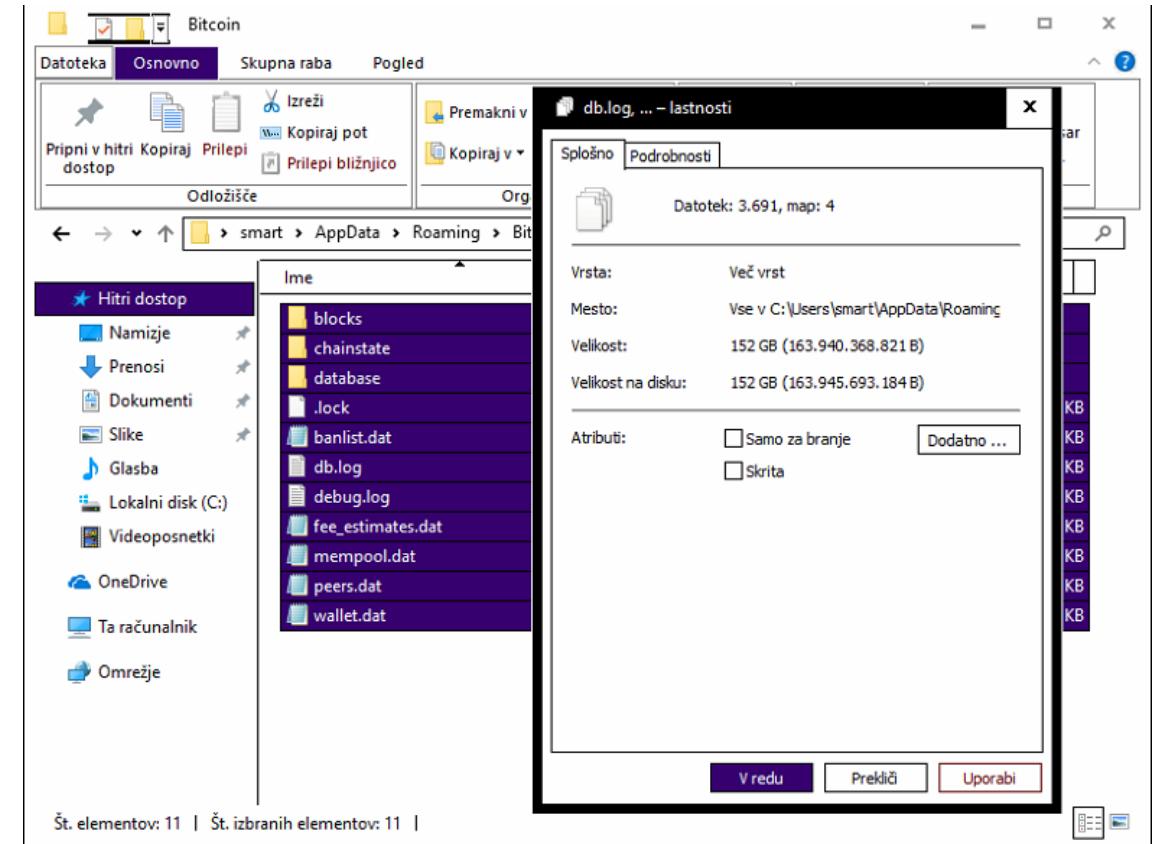
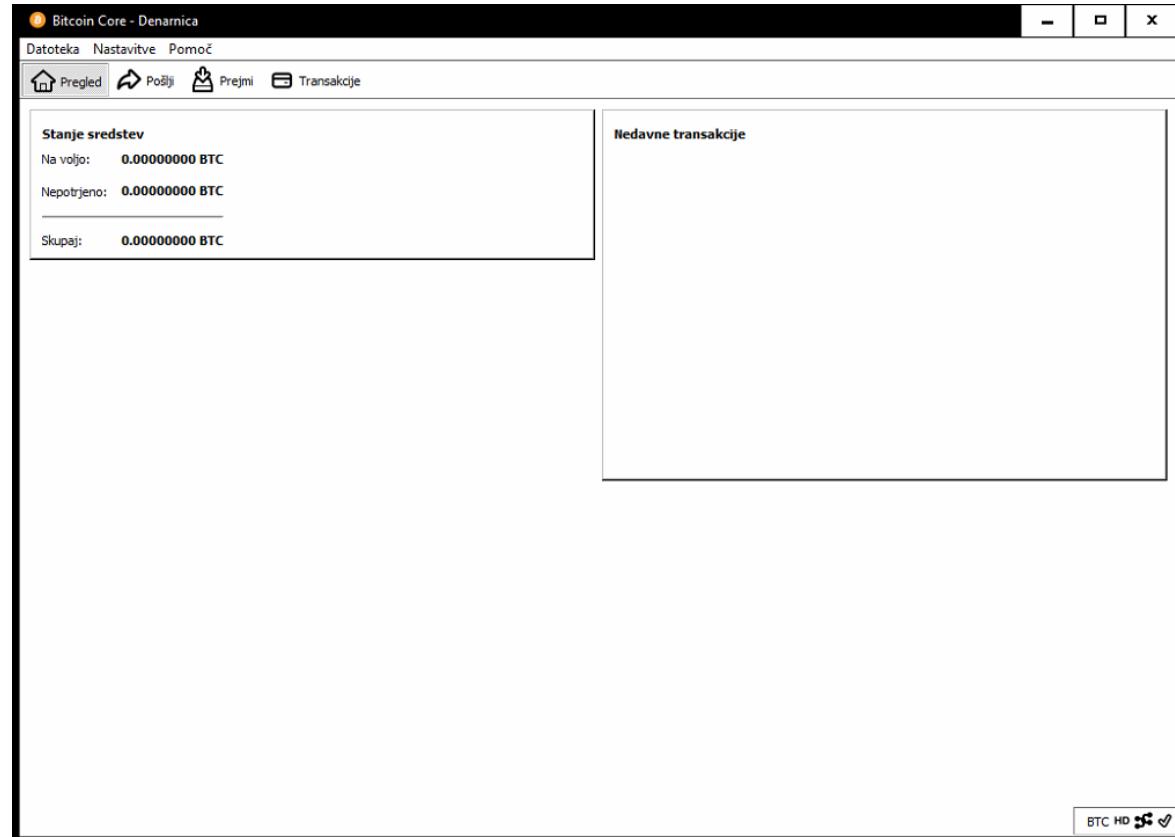
remind elite mobile wave runway obvious
special safe ocean over puzzle gesture

We'll confirm on the next screen.

I've written it down

Namizna/Desktop denarnica

- Popolna kontrola nad vašimi kriptokovanci in zasebnimi ključi
- Možnost povezovanja vaše spletne storitve z denarnico prek RPC ukazov (za napredne uporabnika)



Lahki odjemalec / SPV klient „light wallet“

- Namizni program/aplikacija
- Ni potrebe po prenosu/sinhronizaciji celotne verige blokov (blockchain) saj denarnica zgolj preverja stanje na naslovih
- Preprost izvoz zasebnih ključev za potrebe uvoza v drugo denarnico

Electrum 3.0.2 - default_wallet [standard]



File Wallet View Tools Help

History

Send

Receive

Receiving address 

Description

Requested amount mBTC

Request expires

Save

New



Balance: 0. mBTC



Papirnate denarnice „paper wallet“

- kaj je papirnata denarnica
- v katerih primerih se uporablajo



Pomembni faktorji pri izdelavi papirnate denarnice

- generator/aplikacijo za generiranje zasebnih ključev kriptovalute je potrebno pognati na računalniku brez internetne povezave
 - zaželjeno je da se celotna operacija izvaja na live operacijskem sistemu
 - tiskanje preko USB tiskalnika (tiskalnike priključne na internet odsvetujem)

Strojne denarnice „hardware wallet“

- Najvarnejša metoda hrambe zasebnih ključev kriptovalut
 - Podpora za vodilne kriptokovance
 - Najvišji varnostni standardi v industriji



Izredno pomembno !

- uporaba močnega gesla
- za različne storitve uporablajte različna gesla
- uporaba 2FA (drugo stopenjska avtentifikacija)
- lastništvo nad zasebnimi ključi pomeni lastništvo kripto valute

Gesla

Primer slabega gesla: janeznovak12345



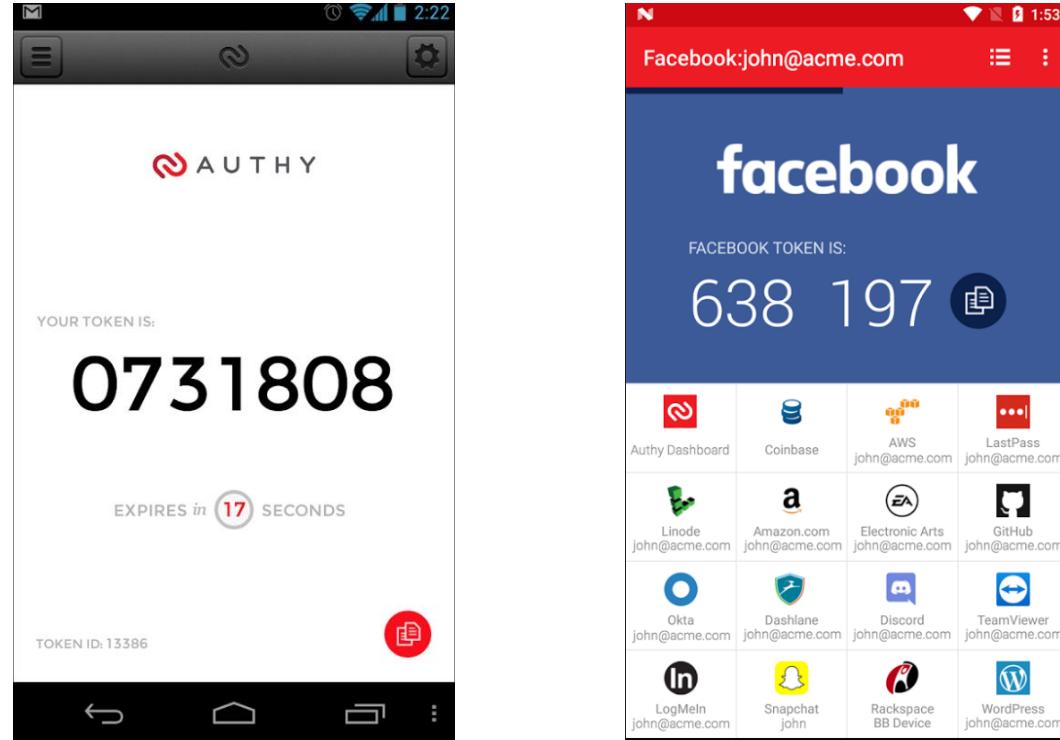
Primer solidnega gesla: !ES@25a2KaJG&



Primer dobrega gesla: CFcphk>QuY9q~5*p



2FA dvostopenjska avtentifikacija



Primer uporabe 2FA @Bitstamp

The screenshot shows the Bitstamp login interface. At the top, there is a navigation bar with links for Home, Account, Buy / Sell, Deposit, Withdrawal, and Tradeview. Below the navigation bar, a dark header bar displays the currency pair BTC / USD and the current exchange rate of USD 10935.00. On the right side of the header bar are links for Register and Log In. The main content area features a "Member Login" form. The form includes fields for User ID (containing "uporabnik") and Password (containing a series of dots). A large blue "Log in" button is centered below the password field. At the bottom of the form, there are links for "Forgot password or ID?" and "Register now for free."

TWO-FACTOR AUTHENTICATION

My Account >

Sub Accounts >

Transactions >

Open Orders >

SMS Price Alerts >

Redeem Coupon >

Mobile Access >

Security >

> Two-Factor Authentication

Withdrawal E-Mail Confirmations

API Access

Password Change Prompts

Settings >

Support >

Verify Account >

Debit Card >

History >

PLEASE WRITE DOWN YOUR AUTHENTICATION KEY:

KJAU4NCQGMYVGRCC

[PRINT IT HERE](#)

DO NOT SAVE THE QR CODE IN ANY DIGITAL FORM. THE QR CODE MUST BE PRINTED ON PAPER AND SAVED IN A SECURE PLACE, WHERE ONLY YOU CAN ACCESS IT.

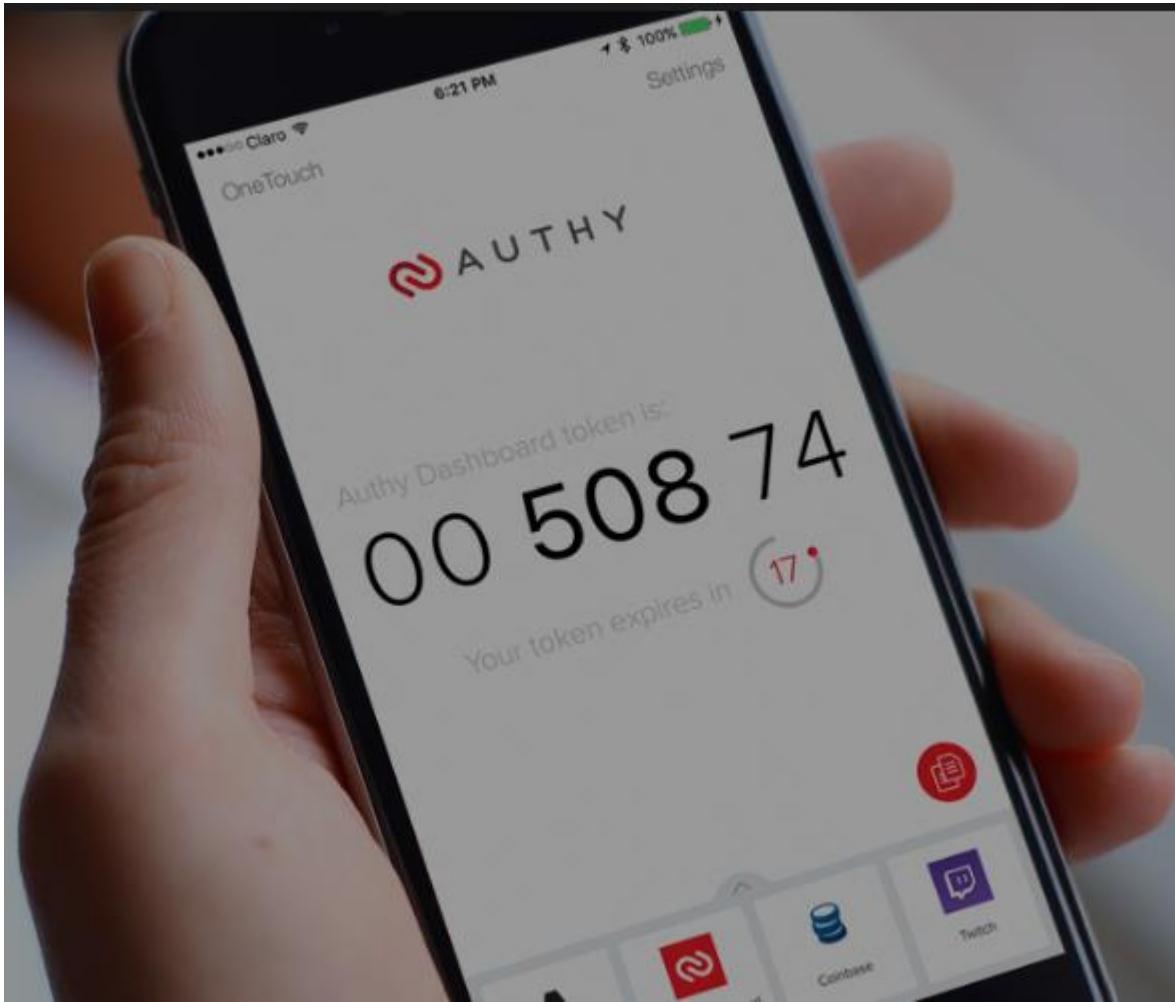
Your Authentication Key:

Insert Your 6-Digit Authentication Code:

IMPORTANT NOTICE

Always write down your authentication key! You will not be able to log in to your account in case you lose your mobile device. If you are having problems with our system rejecting your authentication code, check your mobile device's clock. It must be synchronized perfectly. Your device will generate a new code every 30 seconds.

ENABLE TWO-FACTOR AUTHENTICATION



Two-factor authentication

Invalid authentication code.

[Continue](#)

Lost your device? Check our [two-factor authentication guide](#) or request a two-factor authentication reset [here](#)

Ethereum

- Ethereum denarnice
- Erc20 žetoni in investiranje v ICO

Myetherwallet.com

MYETHERWALLET LLC [US] | <https://www.myetherwallet.com>

DON'T GET PHISHED, please! 🛡 Thank you! ☺

1. BOOKMARK MYETHERWALLET.COM | 2. INSTALL EAL or MetaMask or Cryptonite

3.11.2.3 English Gas Price: 20 Gwei Network ETH (MyEtherWallet)

New Wallet Send Ether & Tokens Swap Send Offline Contracts ENS DomainSale Check TX Status View Wallet Info Help

Create New Wallet

Enter a password

Do NOT forget to save this!

Create New Wallet

This password encrypts your private key. This does not act as a seed to generate your keys. You will need this password + your private key to unlock your wallet.

How to Create a Wallet · Getting Started

Already have a wallet somewhere?

- Ledger / TREZOR / Digital Bitbox : Use your [hardware wallet](#). Your device *is* your wallet.
- MetaMask Connect via your [MetaMask Extension](#). So easy! Keys stay in MetaMask, not on a phishing site! Try it today.
- Jaxx / imToken Use your [Mnemonic Phrase](#) to access your account.
- Mist / Geth / Parity: Use your [Keystore File \(UTC / JSON\)](#) to access your account.

MyEtherWallet.com does not hold your keys for you. We cannot access accounts, recover keys, reset passwords, nor reverse transactions. Protect your keys & always check that you are on correct URL. You are responsible for your security.

The screenshot shows the MyEtherWallet website interface. At the top, there is a red header bar. Below it, the main navigation bar includes a logo, the text "MyEtherWallet", and links for "New Wallet", "Send Ether & Tokens" (which is underlined), "Swap", "Send Offline", and "Contracts". The main content area has a title "- Send Ether & Tokens". Below this, a section asks "How would you like to access your wallet?" and lists several options with radio buttons:

- View w/ Address Only
- MetaMask / Mist
- Ledger Wallet
- TREZOR
- Digital Bitbox
- Keystore / JSON File ?
- Mnemonic Phrase ?
- Private Key ?

At the bottom of this list is another option: "Parity Phrase" with a question mark icon.



Withdraw >

EU Bank (SEPA) >

International Bank >

Bitcoin (BTC) >

Ripple (XRP) >

Litecoin (LTC) >

Ethereum (ETH) > **ETH WITHDRAWAL**

Bitcoin Cash (BCH) >

Debit Card >

IOU (BTC, USD) >

Gold >

WARNING: Please make sure that the receiving party supports Ethereum transactions generated from smart contracts prior to initiating an ETH withdrawal.

I have read the warning

WARNING: Please do not withdraw directly to an ICO address. Always withdraw to your Ethereum private wallet first.

I have read the warning

I AGREE

Vlaganje v etherem ICO projekte

- Sredstev nikoli ne pošiljajte neposredno iz spletne menjalnice, temveč uporabite lastno ethereum denarnico oz ethereum denarnico ki podpira etherum žetone (erc20 standard tokens)
- če denarnice namizna/spletna/mobilna nudi podporo za ethereum, še ne pomeni da podpira erc20 žetone
- Ne pozabite izključno lastništvo nad zasebnim ključem pomeni lastništvo kriptovalute ali kripto žetona

Jaxx

ETH LTC ICN

Receive Send

Your Ethereum Address:
0x670a0eb597c5bd2ba09304eb72dee17c409010dc

ETH
0.00566955
€4.65

Transaction History

Dec 20 2017 10:39 PM Sent To - 0x57...241de -0.09863 ETH

Nov 16 2017 08:39 AM Sent To - 0x0d..ff8e1 -1.2 ETH

Nov 14 2017 10:38 PM Confirmed +0.91598 ETH

Nov 09 2017 02:46 PM Confirmed +0.16931 ETH

Nov 05 2017 05:05 PM Sent To - 0x57...241de -0.03919 ETH

Jaxx

ETH LTC ICN

Receive Send

Your IonomiEthereum Address:
0x670a0eb597c5bd2ba09304eb72dee17c409010dc

ICN
0.0

Transaction History

Feature Not Available

VIEW PRIVATE KEYS

Warning

On the following screen, you'll see a list of your public addresses and private keys generated by your wallet. Your public addresses will be shown on top of your private keys.

Your private keys are the keys to your funds so DO NOT SHARE them with anyone unless you'd like them to have access to your funds.

CANCEL 2 EXPORT

ETHEREUM KEYS

Below are your Ethereum public address and private key pairs.

0.00566955986821545 ETH

Public Key
0x670a0eb597c5bd2ba09304eb72dee17c409010dc

Private Key

0 ETH

Public Key
0xe877448a35fc701cd280476d6594d538f81a3f2e

EXPORT

Vas že boli glava od vseh gesel,
ključev in zaščitnih korakov?

Vse do sedaj je več ali manj brezpredmetno če:

- Ne vzdržujete in posodabljate vašega operacijskega sistema na računalniku/mobilni napravi
- Licenčen protivirusni program je že praktično nujno zlo v digitalni dobi in da tudi za mobilne operacijske sisteme so na voljo
- Če vam zdrava pamet ne narekuje, da se internetnih finančnih ureja na istem računalniku na katerem otroci nameščajo poplavo piratskih iger in programov
- Če vse poprek nameščate nepreverjene aplikacije na vašo mobilno napravo brez vednosti kakšen nivo dostopa do naprave aplikacija ima



Zaupati sebi ali ponudniku storitve?

**Ne preprosto verjeti vsega kar
ste na danes izvedeli !**

**RESEARCH EVERYTHING AND
TRUST YOURSELF FIRST, BEFORE
TRUSTING OTHERS!**

Hvala za vašo pozornost

