PV204 Security technologies

Bitcoin I.

Petr Švenda *svenda@fi.muni.cz* *@rngsec*
Centre for Research on Cryptography and Security, Masaryk University

CROCS
Centre for Research on Cryptography and Security

PREPARATION FOR THE SEMINAR

Preparation: for the seminar

- Pre-install on your desktop
  - Bitcoin Core 24.0.1 (pick zip or gzip file, don't install and don't let it run yet)
    - https://bitcoincore.org/bin/bitcoin-core-24.0.1/
    - Sparrow Wallet https://www.sparrowwallet.com/download/
- Pre-install two wallets on your phone (standard, Lighting)
  - Green: Bitcoin wallet by Blockstream as standard wallet
    - Allows for testnet network option
  - WalletOfSatoshi as Lighting wallet
    - (or BlueWallet/Zap/Muun… if you are more familiar)
  - (Note: these are just recommendations, if you know what you are doing, there are plenty of other options)

Overview

1. Using Bitcoin Core full node (mainnet)
   – Start downloading blocks, investigate connected peers, network
2. Using Bitcoin Core full node locally (regtest)
   – cli, mining, sending, transactions
3. Group discussions – basic Bitcoin questions
4. Getting and sending some (testnet) bitcoins using SparrowWallet

INTRO

Networks in Bitcoin (Mainnet, Testnet, Regtest)

- Mainnet – main, global production network
- Testnet – testing network (global, some mining happens…)
  - Restarted from time to time, contains many different types and versions of TXs
- Regtest – local instance of Bitcoin network
  - Used for local testing (integration, regression,debugging)
  - Blockchain started from block 0, you are the only miner
  - (mined bitcoins unusable on Mainnet)
  - You can insert own transactions, decide on mining new blocks, debug…
- Signet – testing network with not_yet_available features enabled
- Lighting – second layer network atop of Mainnet

P2P Bitcoin network map https://bitnodes.io/

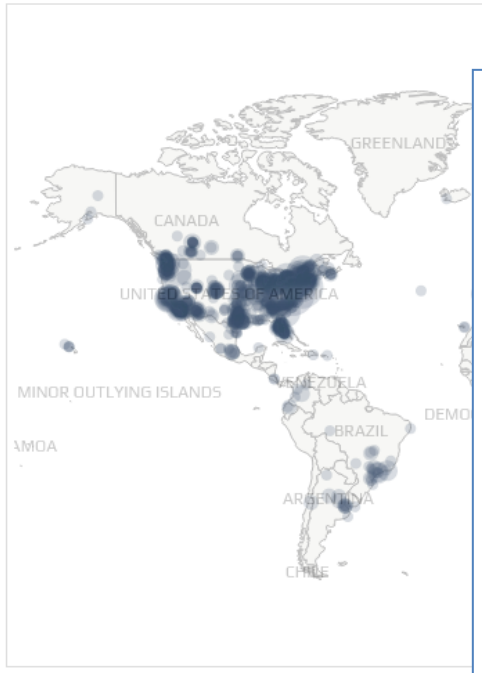
REACHABLE BITCOIN NODES
Updated: Thu Mar 24 09:37:20 2022 CET

15240 NODES CHARTS

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	n/a	8363 (54.88%)
2	United States	1850 (12.14%)
3	Germany	1474 (9.67%)
4	France	528 (3.46%)
5	Netherlands	351 (2.30%)
6	Canada	305 (2.00%)
7	United Kingdom	217 (1.42%)
8	Finland	210 (1.38%)
9	Russian Federation	196 (1.29%)
10	Switzerland	127 (0.83%)

More (86) »



Map shows concentration of reachable Bitcoin noc

BITNODES

Bitnodes estimates the relative size of the Bitcoin peer-to-peer network by finding all of its reachable nodes.

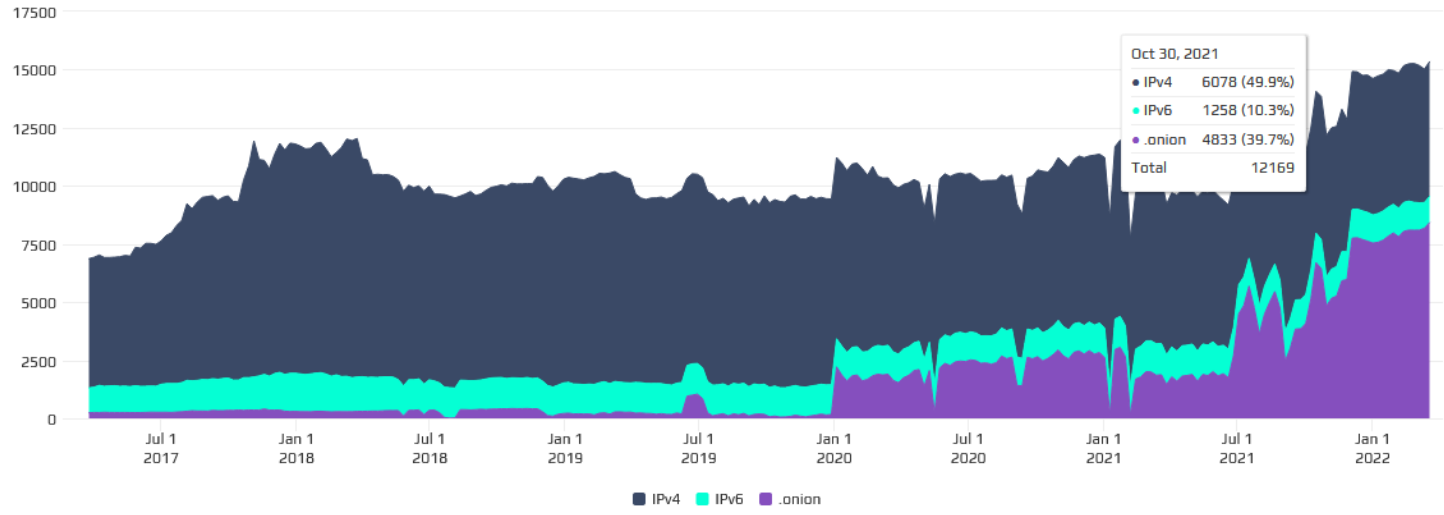
15340 Reachable nodes | 10451 Average | 8472 ▲ 123.35% Since 1825 days ago

NODES

Chart shows the number of reachable Bitcoin nodes during the last 1825 days. Individual series can be enabled or disabled from the legend to view the chart for specific networks.

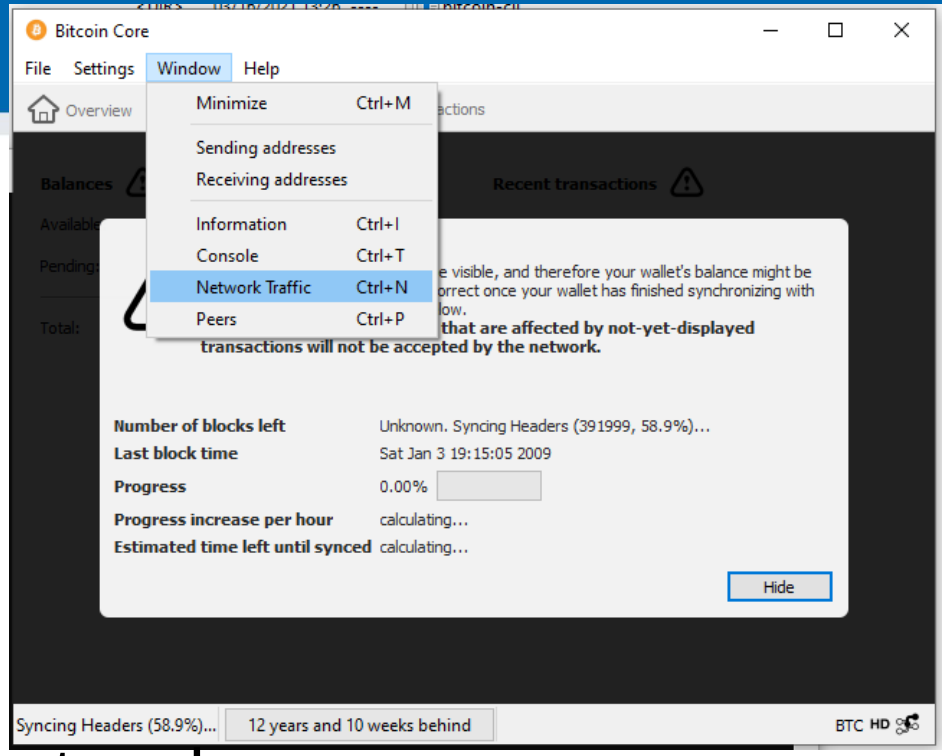
24h 90d 1y 5y

Lo 6868 Hi 15340 Avg 10451 Last 15340 nodes



TASK: USING BITCOIN CORE

Own work: Using API of full node



- Get Bitcoin full node 24.0.1 (pick .zip or .gz)
  - https://github.com/bitcoin/bitcoin/releases
  - https://bitcoincore.org/bin/bitcoin-core-24.0.1/
  - Download and unpack .zip or .gz
- Download few blocks from real Bitcoin P2P network
  - Run bitcoin-qt, Window → Network Traffic (Ctrl+N), Peers (Ctrl+P)
  - Observe and document peers to which you connected (number, version, IP)
- Analyze first few blocks from blockchain
  - Look into Bitcoin/blocks/blk00000.dat (e.g., C:/Bitcoin/blocks/blk00000.dat)
  - If on Windows, Look for bitcoin folder also in your profile
    - c:\Users\your_name\AppData\Roaming\Bitcoin\blocks\

Questions

- Why is your full node connecting to other nodes?
- For how long is the Bitcoin network running now?
- What is the content of first block?
- What is the privacy advantage of sending/querying TXs using your full node?
- How can you compute the current supply of bitcoins?


Lister - [c:\Bitcoin\blocks\blk00000.dat]
File Edit Options Encoding Help
The Times
3/Jan/2009 Chancellor on brink of second bailout for banks

Run strings on already downloaded blocks

- **`strings`** command on Linux
- **`strings`** on Windows: https://docs.microsoft.com/en-us/sysinternals/downloads/strings
- **`c:\Bitcoin\blocks`**`>strings -n 20 *.dat`

TASK: USING BITCOIN-CLI (REGTEST)

Note: Assumed version 24.0.1

```
>bitcoin-cli -regtest getbalance
50.00000000
```

Note: on Windows, do not use PowerShell

Using API: Bitcoin -regtest

- Optional: regtest network blocks are stored in \Bitcoin\regtest\ (Windows) or ~/.bitcoin/regtest (Linux)
  - Run "del /S /Q "%APPDATA%\Bitcoin\regtest\" to erase previous one (on LINUX, remove ~/.bitcoin/regtest)
- Run local network (bitcoin daemon)
  - **`bitcoind -regtest`**
- Create new wallet
  - **`bitcoin-cli -regtest createwallet "testwallet"`**
- Obtain new address for future mined bitcoins (=> **`miner_address`**)
  - **`bitcoin-cli -regtest getnewaddress`**
- Mine 101 blocks: **`bitcoin-cli -regtest generatetoaddress 101`** **`miner_address`**
- Check your balance: **`bitcoin-cli -regtest getbalance`**

This is necessary from 0.20.0 and higher

Using API: Bitcoin -regtest

- Set desired transaction fee BTC/kvB (wallets typically auto computing for you)
  - **`bitcoin-cli -regtest settxfee 0.00002`**
- Send previously mined bitcoins to new address (**`getnewaddress`**→new_address)
  - **`bitcoin-cli -regtest sendtoaddress new_address 10.00`**
- Display info about transaction:
  - **`bitcoin-cli -regtest gettransaction txid`**
- Mine additional to block to include new TX into blockchain…
  - https://bitcoin.org/en/developer-examples, https://bitcoin.org/en/developer-reference#bitcoin-core-apis
- Verify total supply: **`bitcoin-cli -regtest gettxoutsetinfo`**

Questions A.

- What type of address you get via **`getnewaddress`** command?
- How you can distinguish between addresses for mainnet, testnet and regtest?
- Can you send mined regtest bitcoins to mainnet address (e.g., bc1xxxx…)?
- How many bitcoins you are supposed to have after mining 150 blocks? Why **`getbalance`** is showing only 2500 btc?
- How the block reward changes on mainnet? How it changes on regtest net?

TASK: BITCOIN QUESTIONS

Task: collaborative discussion

- Join discussion with group colleagues
- Try to find answers for the questions from the next slides
  - No expectation to do all questions, but cover at least the basic ones
- For every questions:
  - Discuss why and where (usage) it is relevant for Bitcoin (possibly more places)
  - Try to answer using your knowledge, Internet and common sense
  - Use ChatGPT for one marked question
- Note down 2-3 surprising observations to mention to whole classroom

Questions B (you and ChatGPT)

- Answer the question below with your peers
  - How can I pay you 1btc if I have only one UTXO worth of 5btc?
  - What will happen if I will try send double-spending tx to Bitcoin network?
  - Why should you use fresh new address for every receive transaction?
  - What will happen if you create pull request to increasing total number of bitcoins from 21M to 100M at https://github.com/bitcoin/bitcoin?

- Ask ChatGPT the question below, then discuss the answer provided critically
  - What attacks are possible if I'm using Bitcoin wallet which is not connected to my trusted full node?

TASK: USING SIGNATURE COORDINATOR

Bitcoin
P2P network

fullnode

fullnode

Blockchain

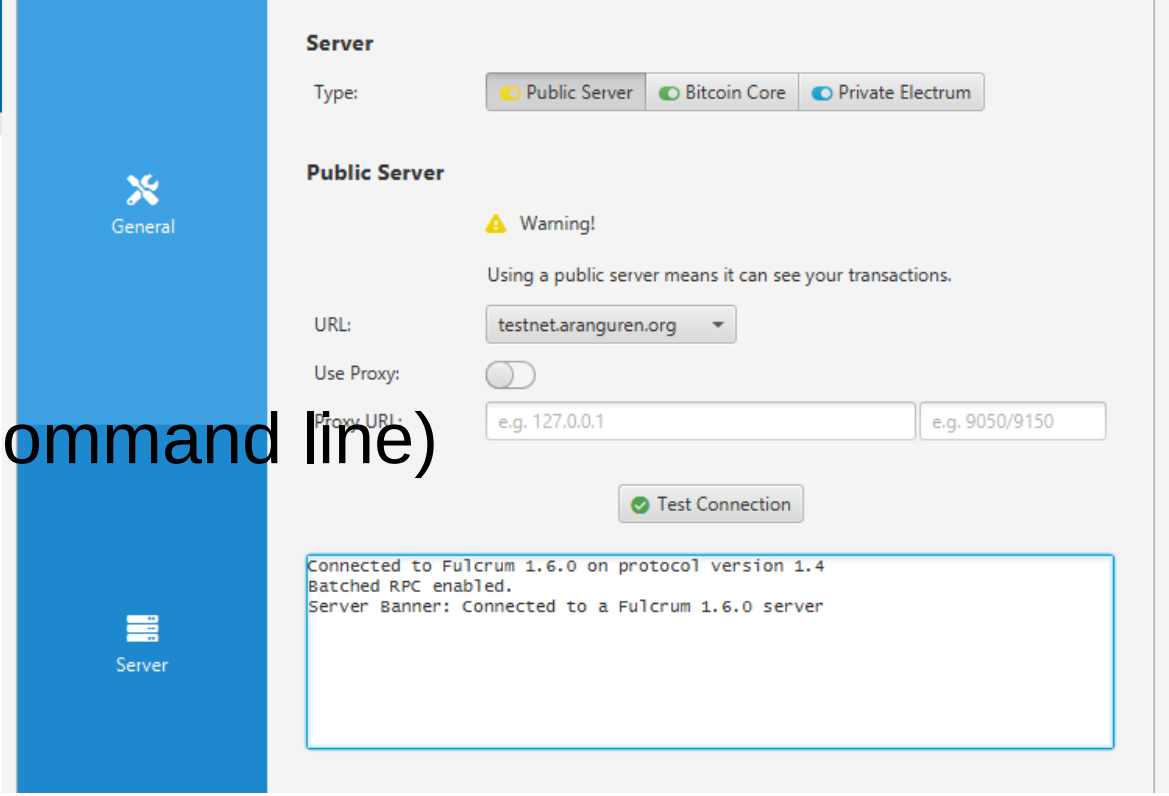
SW-only wallet

With hardware wallet

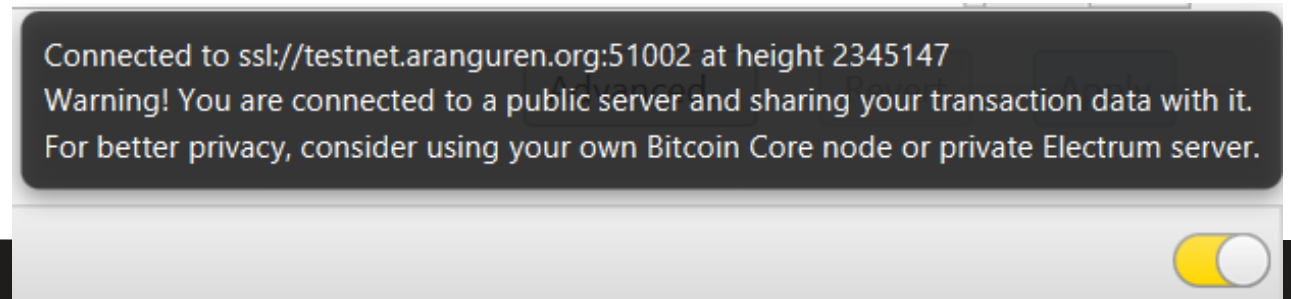
SINGLE-SIGNATURE WALLET (SW-ONLY)

(Examples created for Sparrow 1.6.6)

Starting Sparrow wallet



- Run your wallet with testnet switch (command line)
  - `./sparrow -n testnet`
  - `Sparrow.exe -n testnet`
- Use Public Server option if asked
  - Test Connection to verify connectivity
  - Can be changed later File → Settings
- (Bitcoin Core and Private Electrum are more private options)
  - You would be connecting to your own fullnode (but you must have one ☺)
- Check that you are online
  - (right bottom)

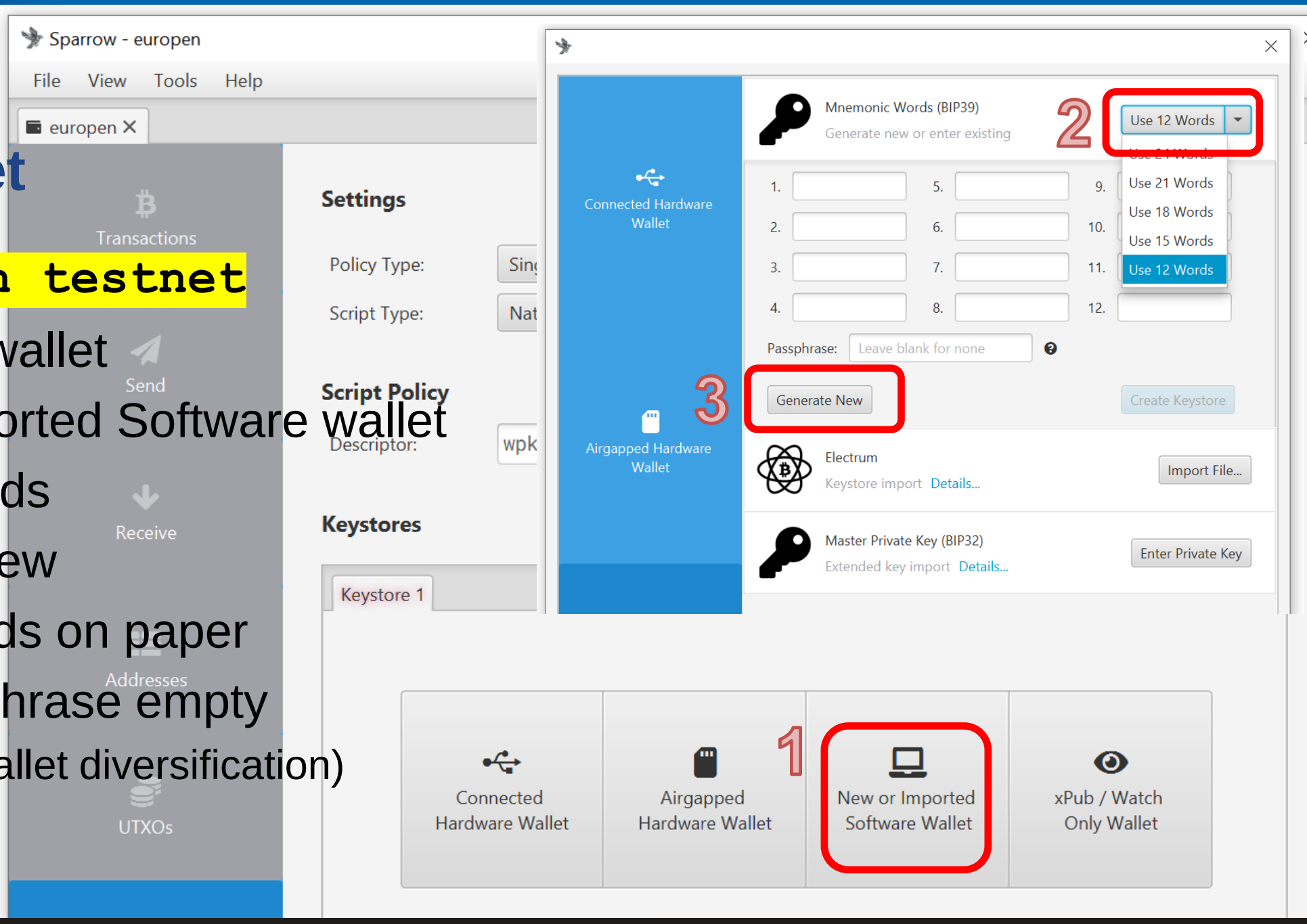


Create wallet

- `sparrow -n testnet`
- File → New wallet

1. New or Imported Software wallet
2. Use 12 Words
3. Generate New

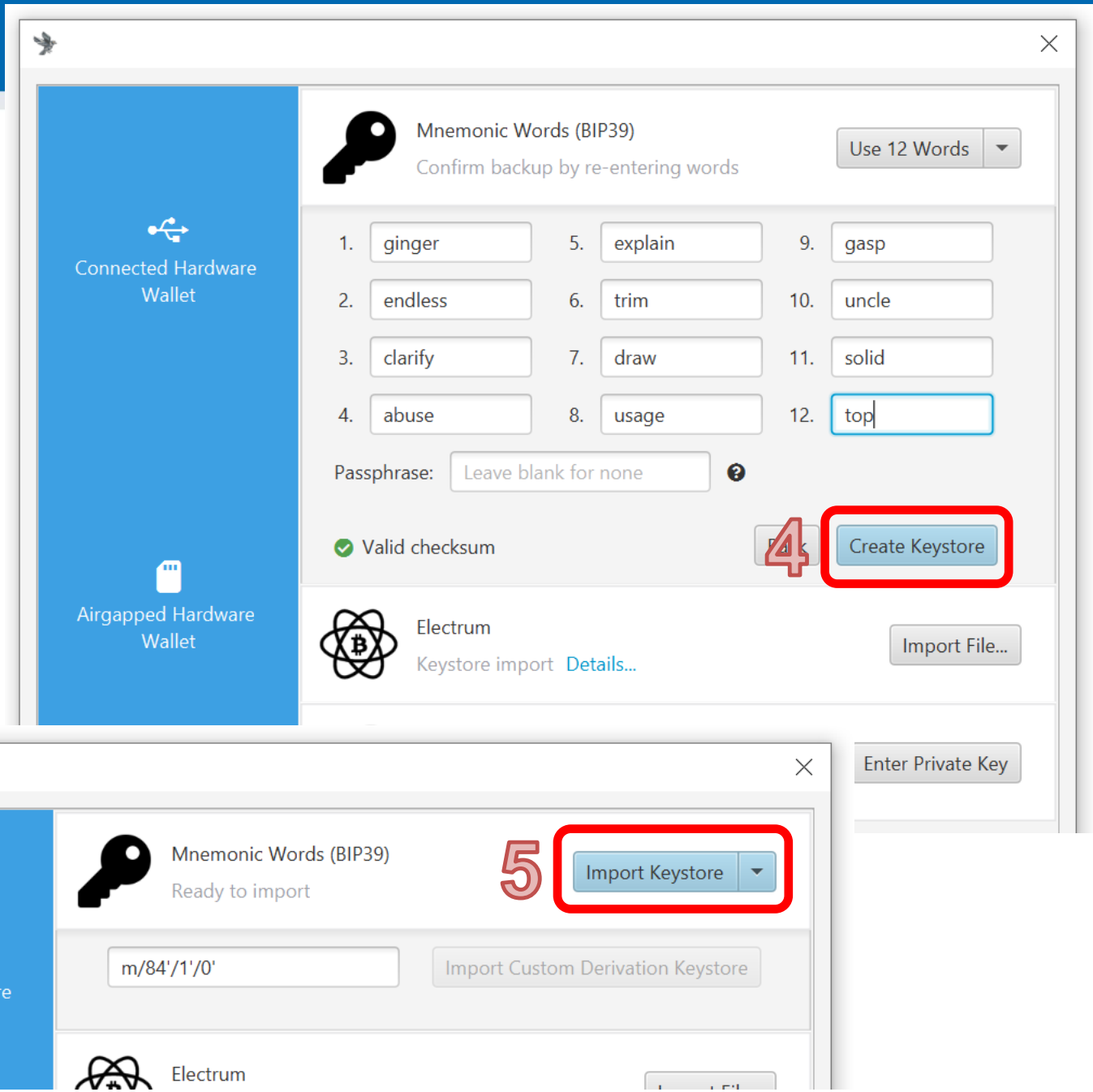
- Write 12 words on paper
- Leave Passphrase empty
  - (additional wallet diversification)



Create wallet

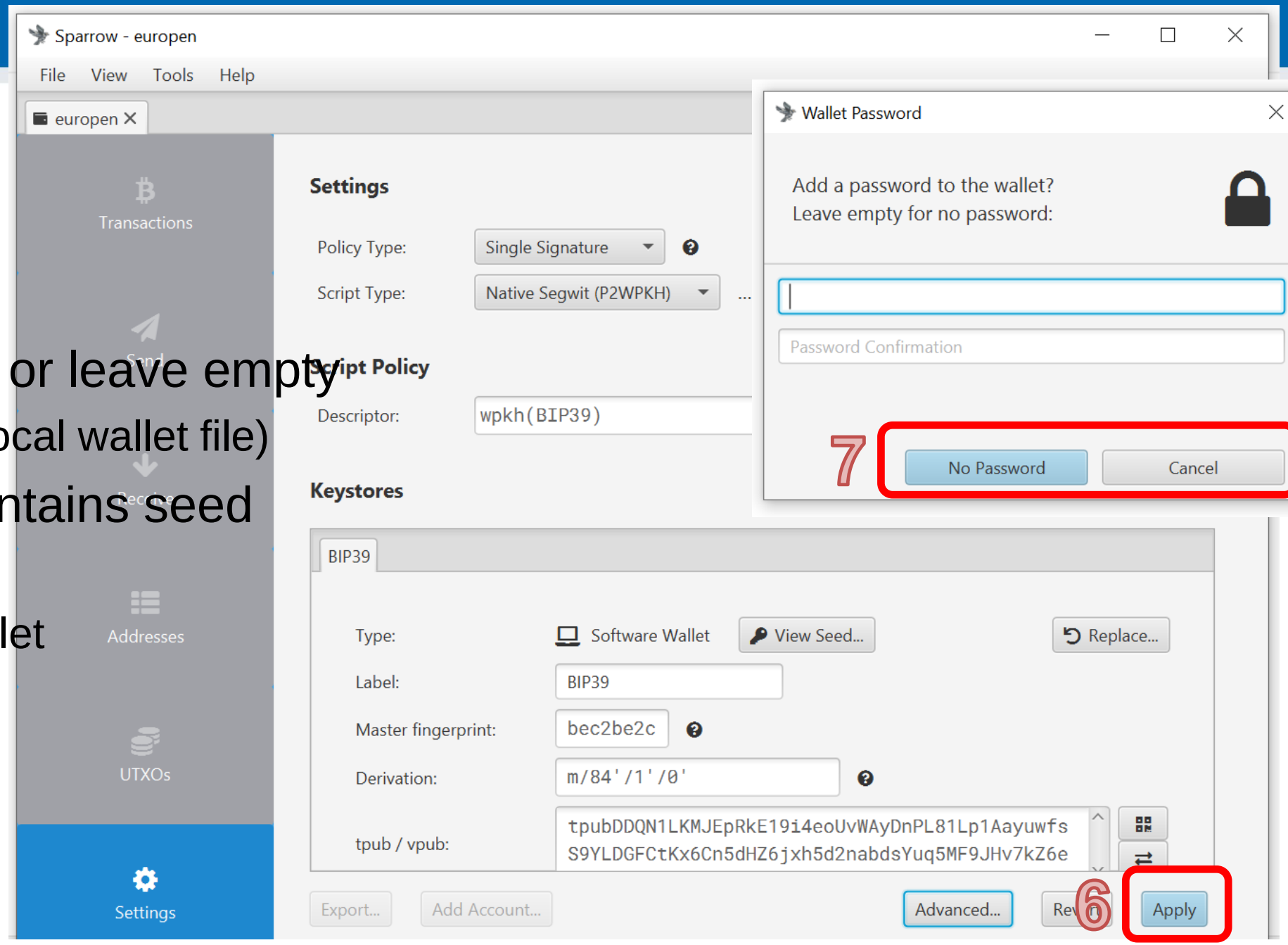
4. Create Keystore
- Confirm backup
- Reenter words

5. Import Keystore

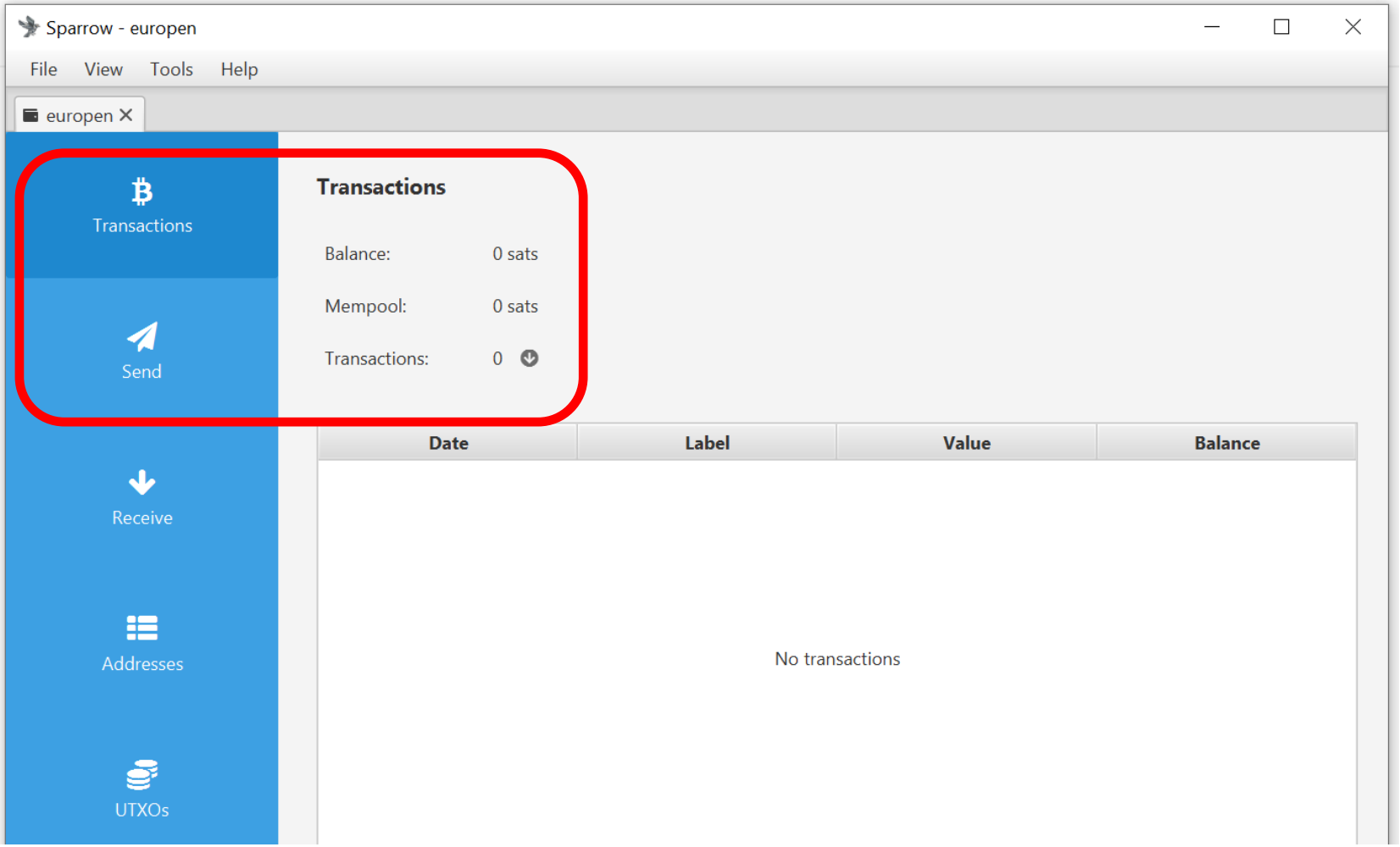


Create wallet

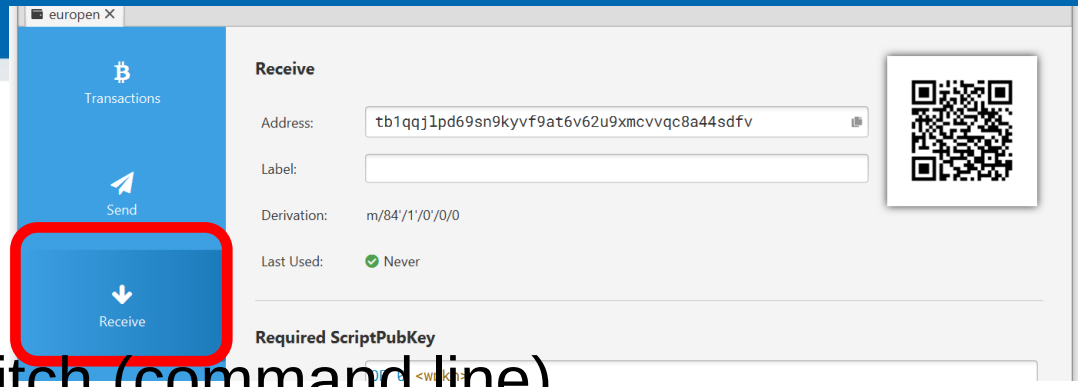
6. Apply
7. Set password or leave empty
   - (encryption of local wallet file)
- Local wallet contains seed
  - *.mv.db file
  - File→Open wallet



Wallet created (but empty ☺)



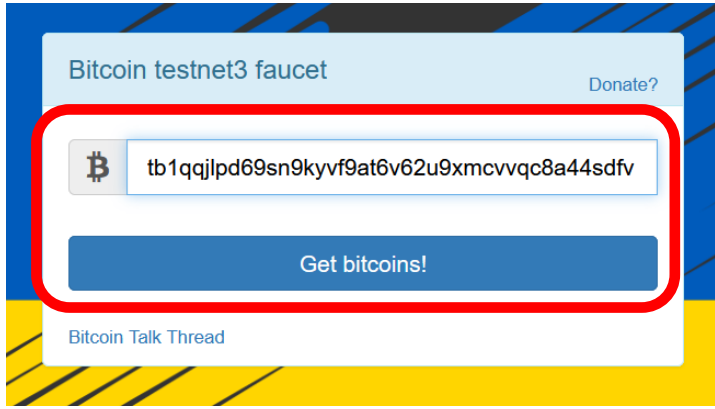
Getting test bitcoins (tBTC)



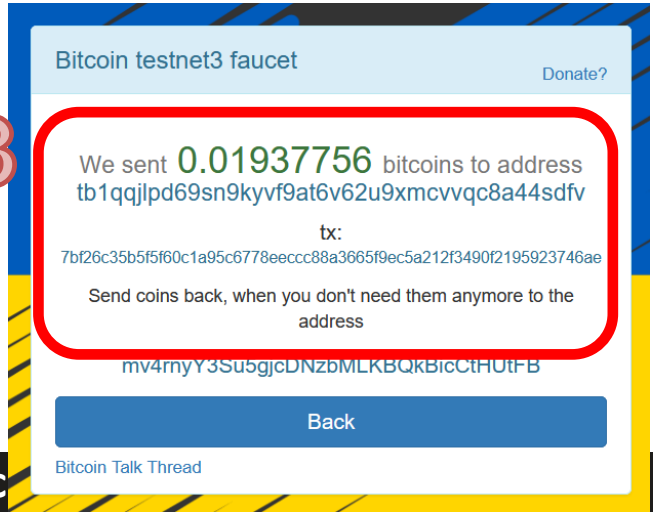
1

- If not running, run your wallet with testnet switch (command line)
  - E.g., **`./sparrow -n testnet`**
  - Generate new (testnet) receive address
- Go to https://coinfaucet.eu/en/btc-testnet/
  - If doesn't work use https://testnet-faucet.com/btc-testnet/
  - Insert your testnet receive address
  - You may get more every 12 hours (per single IP)
  - (but please don't abuse)
- Check your tx: https://mempool.space/testnet
- Testnet TX explorer: https://blockstream.info/testnet/
  - Software visualizing blockchain

2

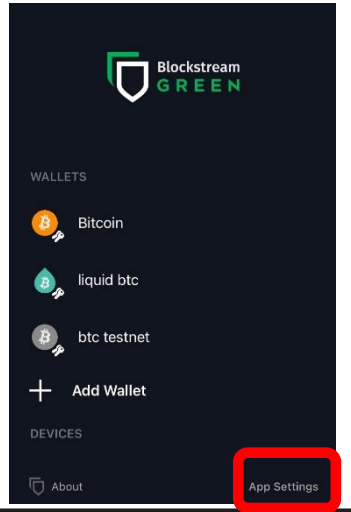


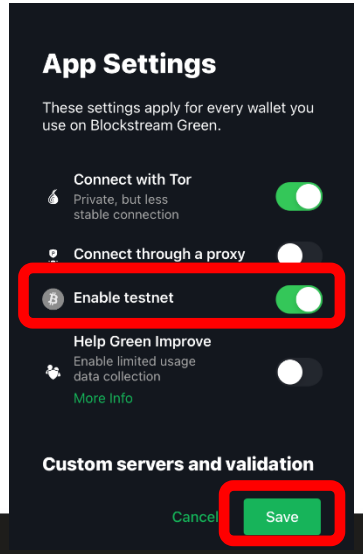
3

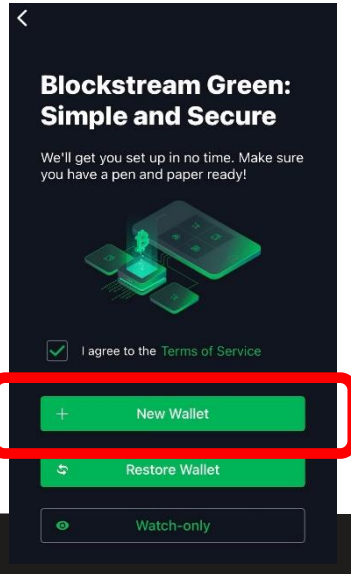


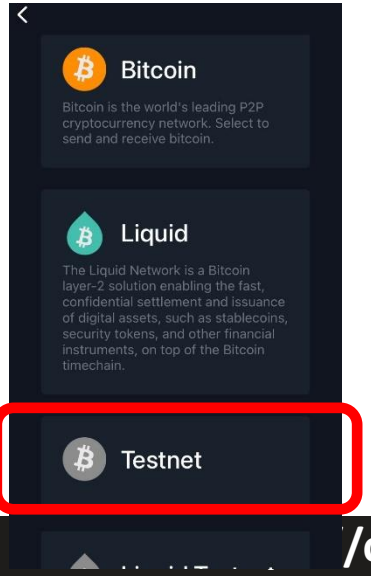
Get mobile wallet

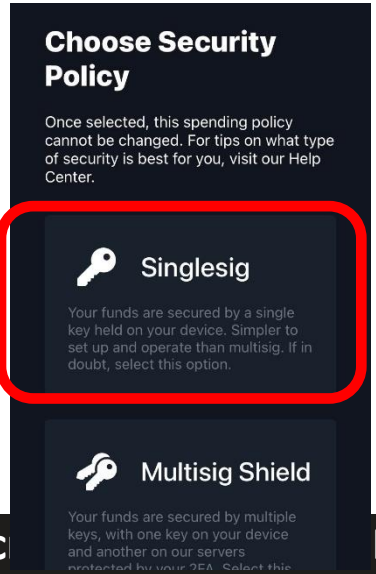
- Get Green wallet by Blockstream on your mobile phone
  - https://apps.apple.com/us/app/green-bitcoin-wallet/id1402243590
  - https://play.google.com/store/apps/details?id=com.greenaddress.greenbits_android_wallet&hl=en&gl=us)
  - Pick testnet option
- Try send between to Green and Sparrow









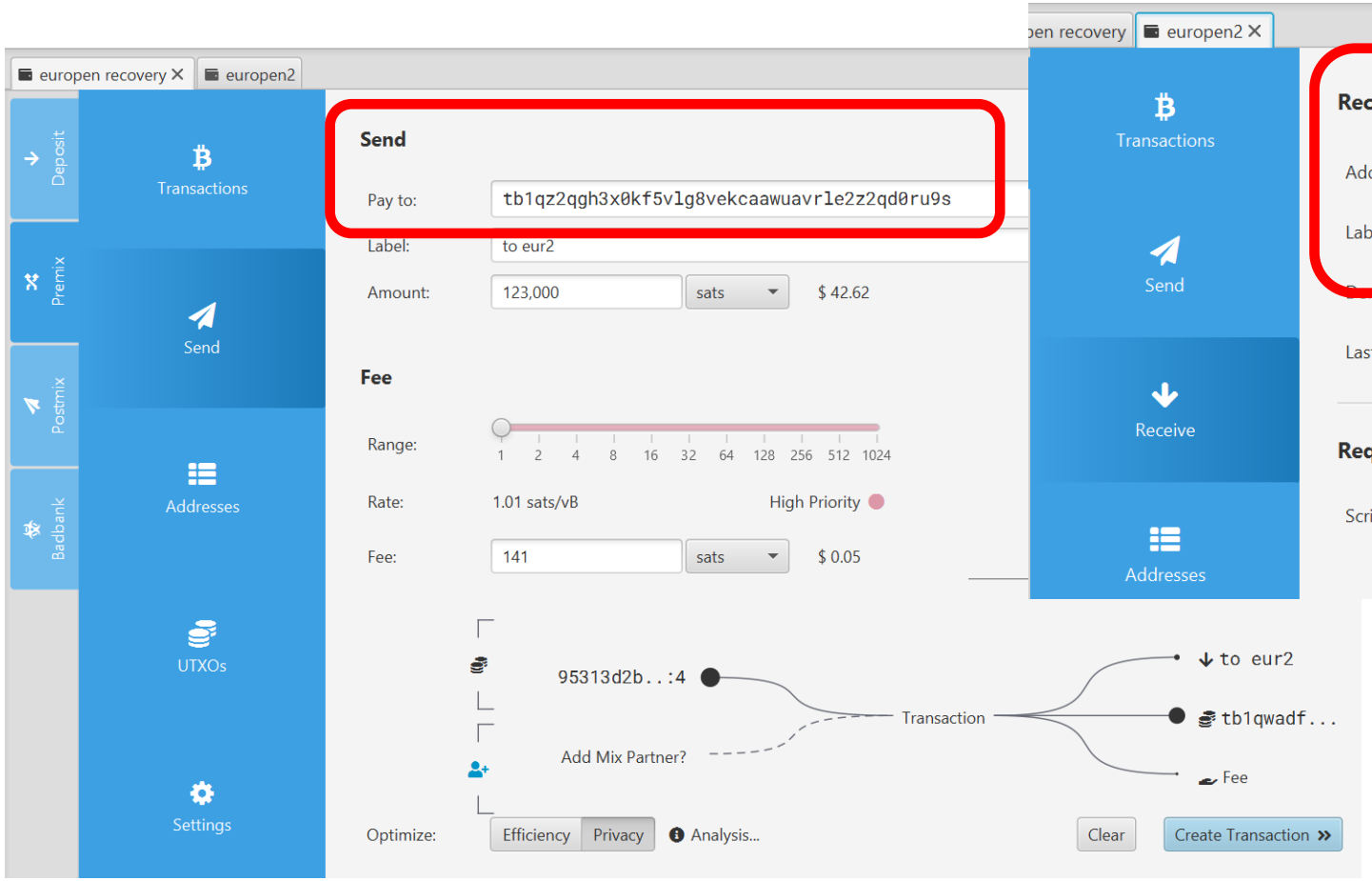


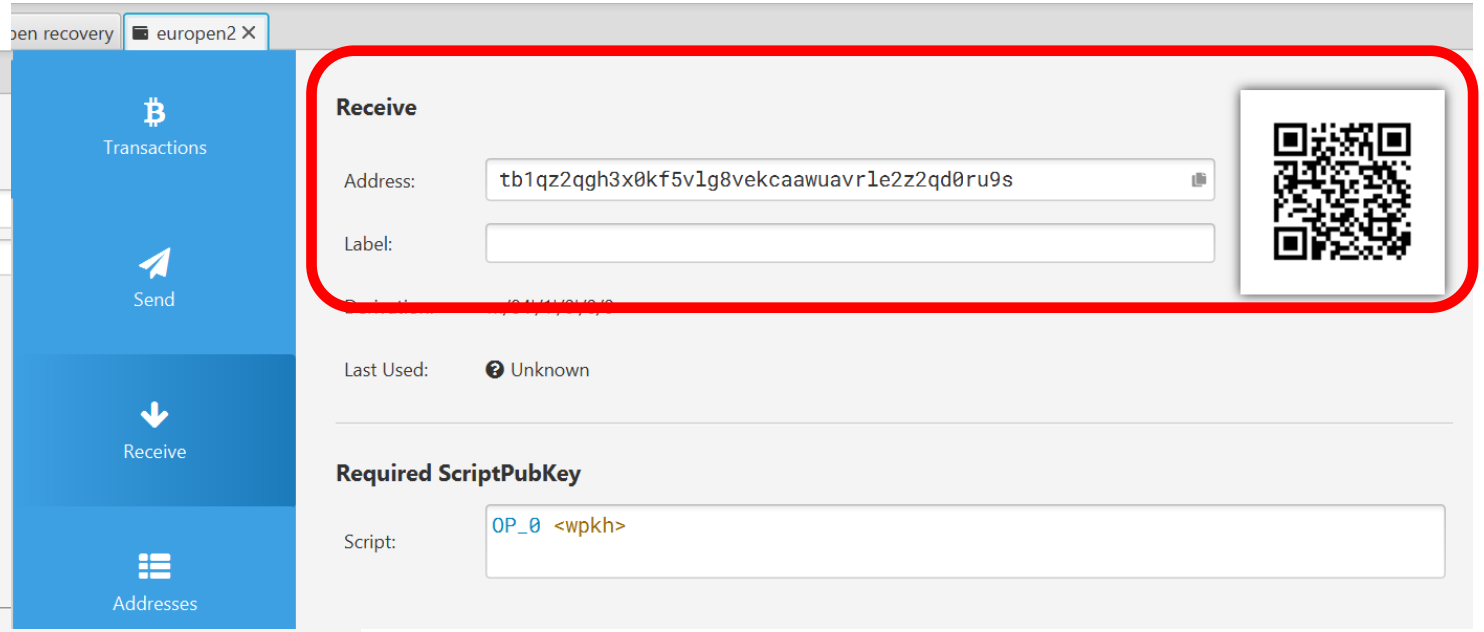
Task: send some tBTC to your peer

- Select one of your neighbors as peer (PC1 and PC2)
- Obtain his/her receive address
  - Via messenger: PC2 → Receive tab → Copy address → send via Signal → PC1
  - Via QR: PC2 → Receive tab ; PC1 → Send → camera icon → scan address QR
- Enter some sats into Amount box
  - Observe visualized transaction below (more inputs may be added)
- Try again, but now with manual coin selection
  - UTXO tab → select one or more → Send Selected

PC1

PC2


europen recovery
europen2
Deposit
Premix
Postmix
Badbank
Transactions
Send
Addresses
UTXOs
Settings
Send
Pay to:
tb1qz2qgh3x0kf5vlg8vekcaawuavrle2z2qd0ru9s
Label:
to eur2
Amount:
123,000
sats
$ 42.62
Fee
Range:
1 2 4 8 16 32 64 128 256 512 1024
Rate:
1.01 sats/vB
High Priority
Fee:
141
sats
$ 0.05
95313d2b..:4
Add Mix Partner?
Transaction
to eur2
tb1qwadf...
Fee
Optimize:
Efficiency
Privacy
Analysis...
Clear
Create Transaction


europen2
Transactions
Send
Receive
Addresses
Receive
Address:
tb1qz2qgh3x0kf5vlg8vekcaawuavrle2z2qd0ru9s
Label:
Last Used:
Unknown
Required ScriptPubKey
Script:
OP_0 <wpkh>

Task: attack your setup! (15 mins)

- Imagine five different ways how you (as an attacker) can steal funds from Sparrow single signature wallet of your colleague
  - Write it into Miro: https://miro.com/app/board/uXjVPaI0Mp4=/?share_link_id=697987574971
    - Password: ‘fimunicz’
  - Be creative, assume weak but also powerful attacker (thief, organizations, manufacturer..)
  - Discuss the cost and prerequisites of the different attacks
- For each attack, describe how availability of secure element may help
  - What functionality of secure element is required?

(Look for your testnet txs from bitcoin core client)

- We send testnet tBTC => there must be corresponding transaction
- Can we look it on our own fullnode (bitcoin-qt we used previously)?
- Possible, but you need to download whole testnet3 blockchain
  - Files are located in \Bitcoin\testnet3\
- When searching for transaction (locally), use --testnet switch
  - **`bitcoin-cli -testnet`**

No assignment this week ☺

HOW MANY QUESTIONS YOU KNOW ANSWER TO?

Questions: Basics

- How can you get some bitcoin(s)? (At least three different options)
- How can I pay you 1btc if I have only one UTXO worth of 5btc?
- Can you get less than 1 bitcoin?
- Can you reverse bitcoin payment if send to wrong address?
- Why “Not your keys, not your bitcoin”? What is non-custodial wallet?
- How can someone steal your bitcoins? (At least three different options)
- For what reason are miners consuming a lot of energy?
- How frequently is new block with transactions included to blockchain?
- What will happen if I will try send double-spending tx to Bitcoin network?
- If I will send you bitcoin on-chain, can you tell from whom I got it?
- What is the current inflation rate of Bitcoin? What will it be in May 2024? Why?

Questions

- Why should you use fresh new address for every receive transaction?
- Why is theoretical maximal limit of on-chain transactions ~6-7tx/sec?
- How is it possible to perform 1000tx/sec between two users (today)?
- When will all bitcoins be mined? What will happen then with mining?
- What will happen if one miner controls 51% of hashrate?
- Why is Bitcoin network not flooded (DOSed) with invalid transactions?
- Can Bitcoin operate without the Internet?
- What is difference between soft- and hard- fork? Why is Bitcoin always aiming for soft-forks only?

Questions

- What will happen if you create pull request to increasing total number of bitcoins from 21M to 100M at https://github.com/bitcoin/bitcoin?
- What will happen if such code change is accepted by Bitcoin core developer?
- Can I operate full Bitcoin node without owning any bitcoin?
- Can you receive bitcoins without operating full node?
- What attacks are possible if I'm using Bitcoin wallet which is not connected to my trusted full node?
- What will happen if someone manages to compute SHA256 with specified number prefix zeros (mining puzzle) 1000x faster than now?

Questions

- What will happen to Bitcoin security if quantum computer powerful enough to break 256b ECC is build?
- When will Proof of Stake replace Proof of Work in Bitcoin?
- What is a difference between public key and Bitcoin address?
- What ECC curve is used for Bitcoin?
- What happens when private key for some UTXO is permanently lost?
- How you can you make your relatives to inherit your bitcoins?
- Why is open-source important for Bitcoin to work?

Questions

- How high fee is required for transaction to be included to block?
- What information is one leaking when browsing transactions using 3rd party block explorers?
- Why is coinbase transaction (miner's reward) spendable only after 100 blocks?