Gymnázium Zlín

Bitcoin basics

https://crocs.fi.muni.cz/papers/btc

Petr Švenda ✉ ***svenda@fi.muni.cz*** ***@rngsec***
with help from Antonín Dufka, Lukasz Chmielewski
Centre for Research on Cryptography and Security, Masaryk University

CROCS
Centre for Research on
Cryptography and Security

WHY BITCOIN?

Especially if you are not interested in Bitcoin.

“Bitcoin fixes everything!”

https://twitter.com/DominicFrisby/status/1388448025970884609

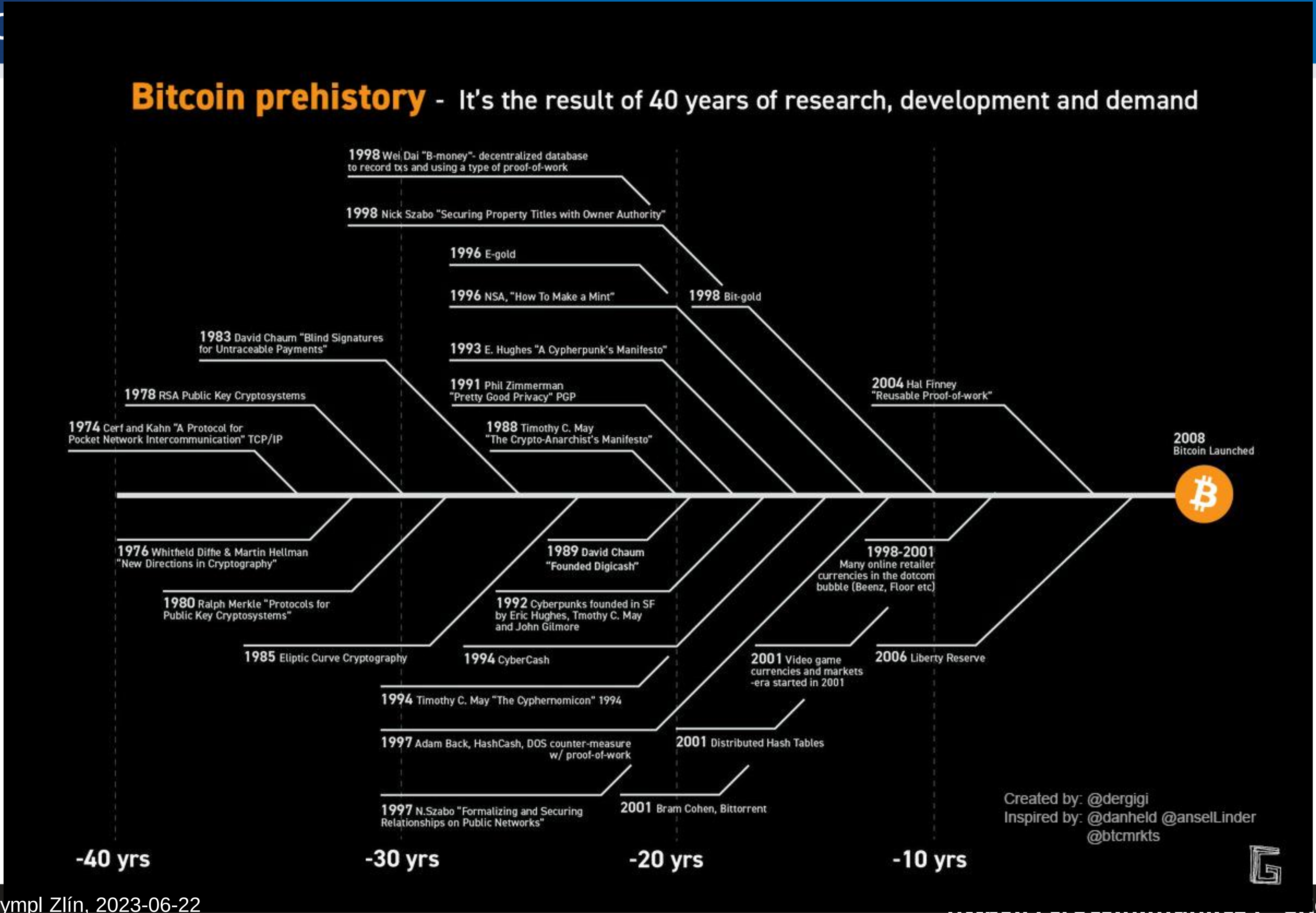
Goals for this tutorial

Important questions we will NOT cover: Lighting network, mining enviro impact, OP_RETURN, price volatility, altcoins tech… – great topics for chat afterwards! 🍺

- Bitcoin does not fix everything, but is on a frontline
  - – No safety net, no chargeback, attacker anonymous => security technique must really work, great for battle-testing security ideas, natural “bug bounty program”
- 6 main tech pieces we will cover (also usable outside Bitcoin world)

1. How to backup key(s) (single seed, BIP39, Shamir)
2. ~~How to make always fresh keys (derivation via BIP32~~, also address privacy)
3. ~~How to protect signing key against malware~~
   - (multisig, hardware wallet, airgap pc + tx bi
4. ~~How to introduce restricted signing policy (ti~~
5. ~~How to protect your financial privacy (CoinJo~~ ,)
6. ~~How to use hardware wallet with secure element~~

If interested in more details about Bitcoin usage tutorial, visit https://crocs.fi.muni.cz/papers/btc



Bitcoin prehistory - It's the result of 40 years of research, development and demand

1998 Wei Dai "B-money"- decentralized database to record txs and using a type of proof-of-work

1998 Nick Szabo "Securing Property Titles with Owner Authority"

1996 E-gold

1996 NSA, "How To Make a Mint"

1998 Bit-gold

1983 David Chaum "Blind Signatures for Untraceable Payments"

1993 E. Hughes "A Cypherpunk's Manifesto"

1978 RSA Public Key Cryptosystems

1991 Phil Zimmerman "Pretty Good Privacy" PGP

2004 Hal Finney "Reusable Proof-of-work"

1974 Cerf and Kahn "A Protocol for Pocket Network Intercommunication" TCP/IP

1988 Timothy C. May "The Crypto-Anarchist's Manifesto"

2008 Bitcoin Launched

1976 Whitfield Diffie & Martin Hellman "New Directions in Cryptography"

1989 David Chaum "Founded Digicash"

1998-2001 Many online retailer currencies in the dotcom bubble (Beenz, Floor etc)

1980 Ralph Merkle "Protocols for Public Key Cryptosystems"

1992 Cyberpunks founded in SF by Eric Hughes, Tmothy C. May and John Gilmore

1985 Eliptic Curve Cryptography

1994 CyberCash

2001 Video game currencies and markets -era started in 2001

2006 Liberty Reserve

1994 Timothy C. May "The Cyphernomicon" 1994

1997 Adam Back, HashCash, DOS counter-measure w/ proof-of-work

2001 Distributed Hash Tables

1997 N.Szabo "Formalizing and Securing Relationships on Public Networks"

2001 Bram Cohen, Bittorrent

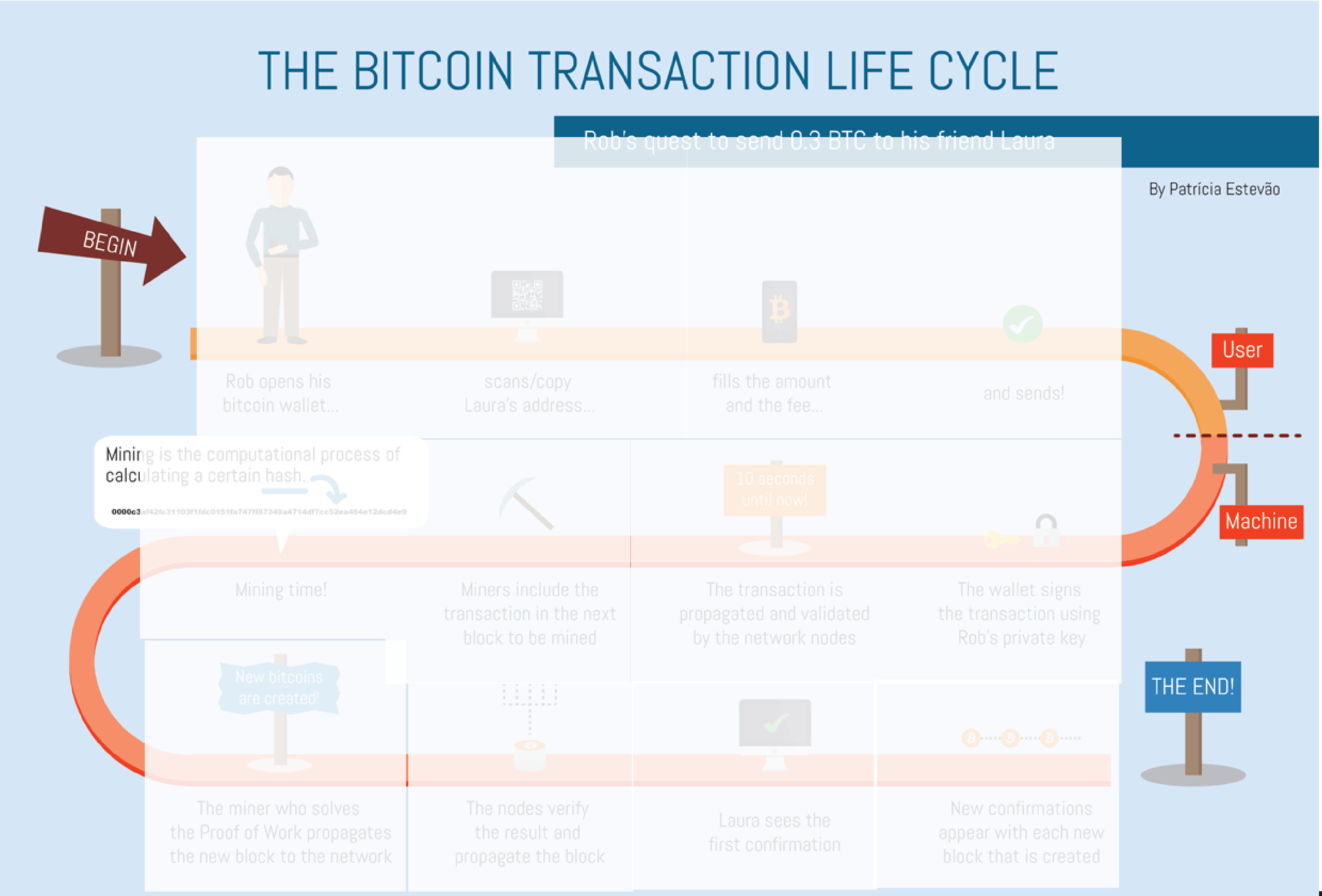
Created by: @dergigi
Inspired by: @danheld @anselLinder @btcmrkts

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

BASICS

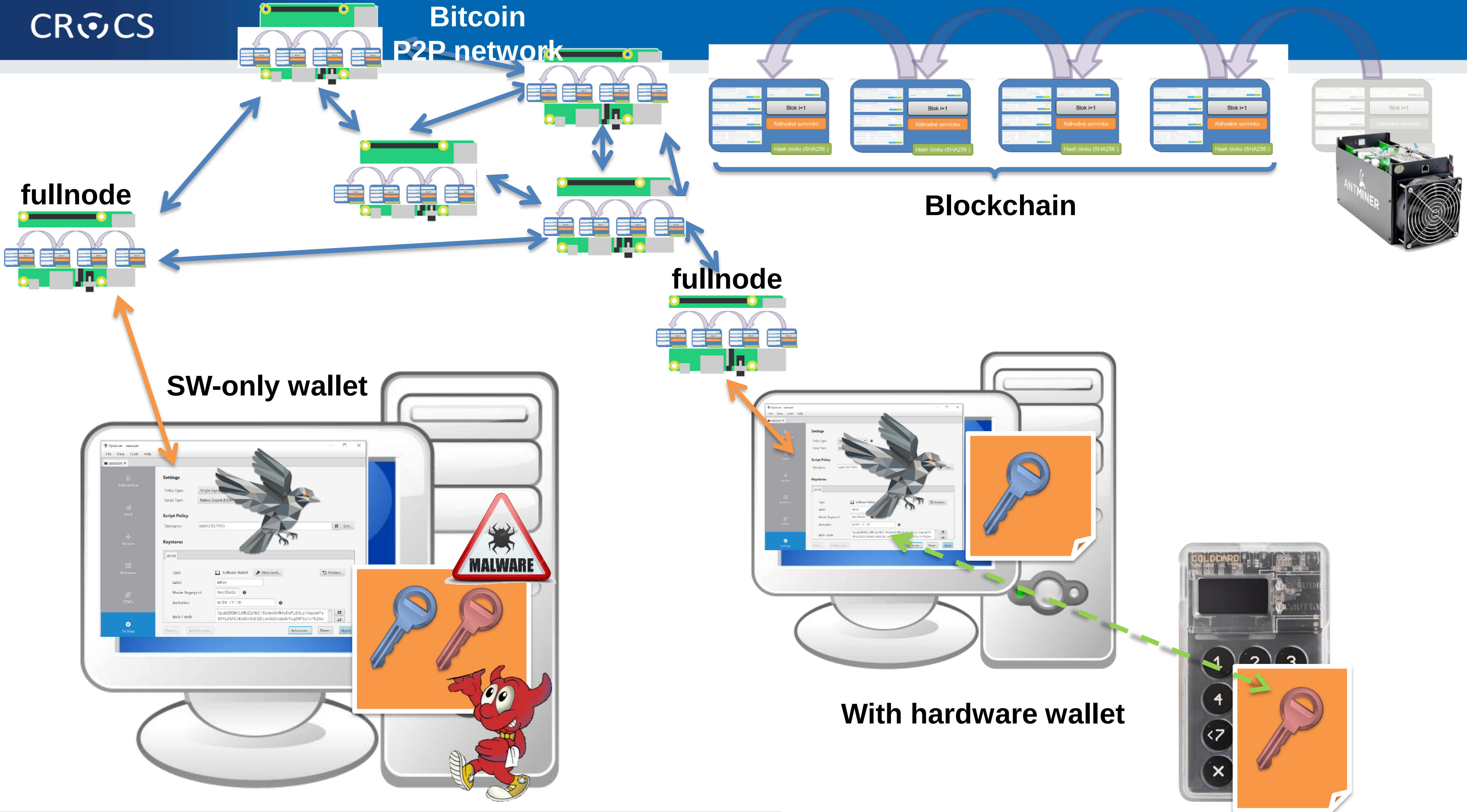
https://livebitnews.com/wp-content/uploads/2017/09/bitcoin-transaction-life-cycle-high-resolution-1.png


THE BITCOIN TRANSACTION LIFE CYCLE
Rob's quest to send 0.3 BTC to his friend Laura
By Patrícia Estevão
BEGIN
Rob opens his bitcoin wallet...
scans/copy Laura's address...
fills the amount and the fee...
and sends!
User
Machine
Mining is the computational process of calculating a certain hash.
0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9
Mining time!
Miners include the transaction in the next block to be mined
10 seconds until now!
The transaction is propagated and validated by the network nodes
The wallet signs the transaction using Rob's private key
New bitcoins are created!
The miner who solves the Proof of Work propagates the new block to the network
The nodes verify the result and propagate the block
Laura sees the first confirmation
New confirmations appear with each new block that is created
THE END!

- Wallet
- Address
- Fee
- Transaction
- Signing
- Network nodes
- Block
- Mining
- Proof of Work
- Verification
- Block reward
- Tx confirmation
- And many more…

Main design goals of the Bitcoin

1. Decentralization
   - No central authority or intermediary (=> no single point of failure), possibility of self-custody
   - No limitation on network participants (no permission to join is required)
   - Applies to executing a transaction, but also development, infrastructure, mining…
2. Transparency
   - All transactions recorded on public ledger; validity of every “bitcoin” easy to verify
   - Total number of bitcoins in circulation easy to assess (monetary policy, fixed supply)
3. Security based on cryptography (mainly signature, hash functions)
   - Ownership of bitcoins proved only cryptographically (no “chargeback” based on human decision)
   - Protection of bitcoins reduced to protection of private key(s)
4. Pseudonymity of participants
   - bitcoins connected to public keys, not usernames (does not automatically mean anonymity!)



Bitcoin P2P network

fullnode

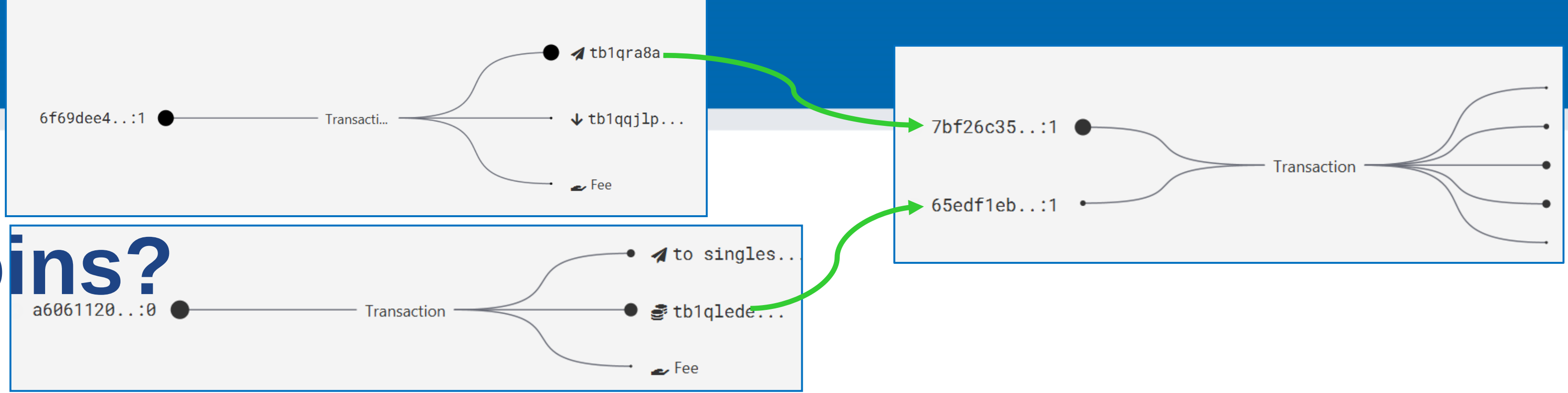
Blockchain

fullnode

SW-only wallet

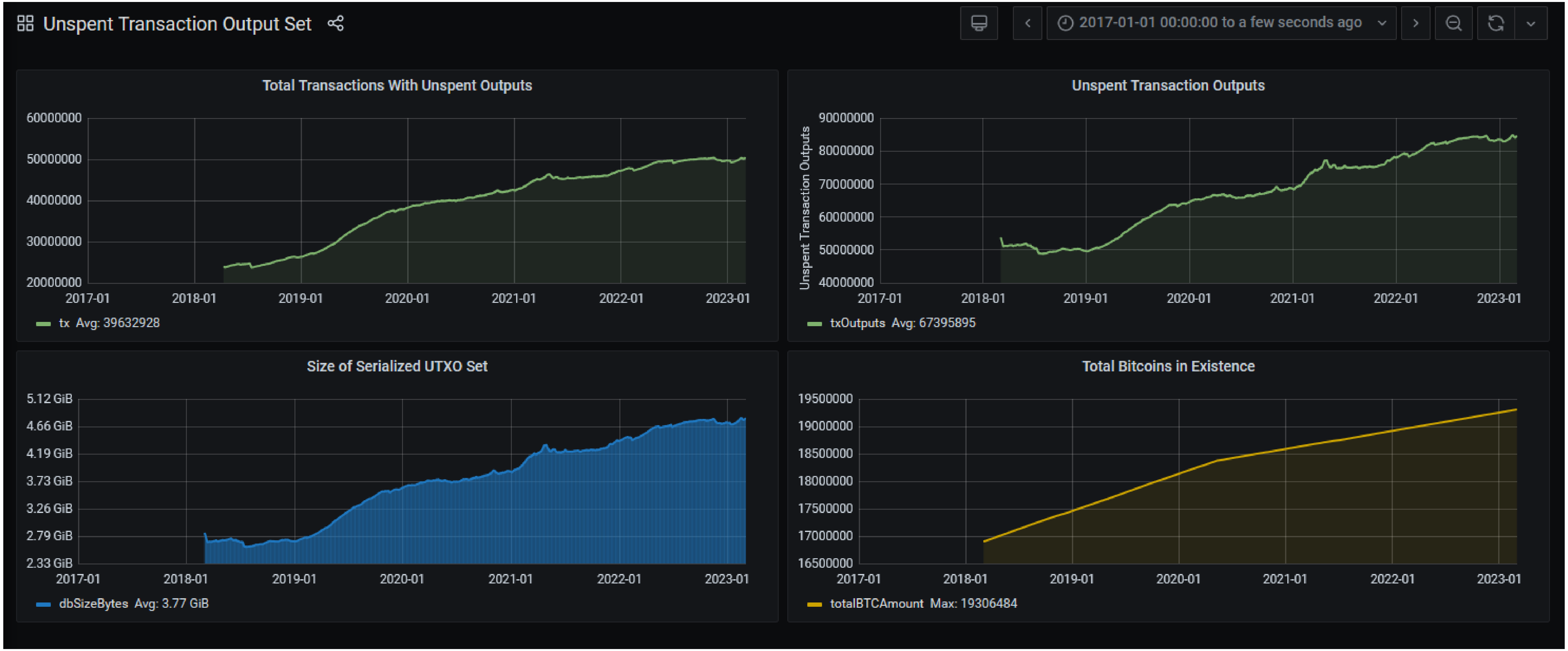
With hardware wallet

Where are my bitcoins?



- Public ledger of all transactions (blockchain)
  - Propagated between Bitcoin fullnodes (P2P network)
- “Bitcoin holdings” - sum of values of not-yet-spent transactions control
  - Unspent Transaction Output (UTXO)
- “Bitcoin send” – take “your” UTXO and use it as input to new one
  - Specify recipient by script specifying what must be done int future send (lockscript)
  - Typical lockscript is “prove that you can sign with private key corresponding to THIS public key”
- “Bitcoin receive” – generate variable part of lockscript (public) and share with sender + monitor blockchain for my transaction
- Protection and handling of private keys is paramount
  - “Not your keys, not your bitcoin! “

UTXO set = all currently valid “bitcoins”

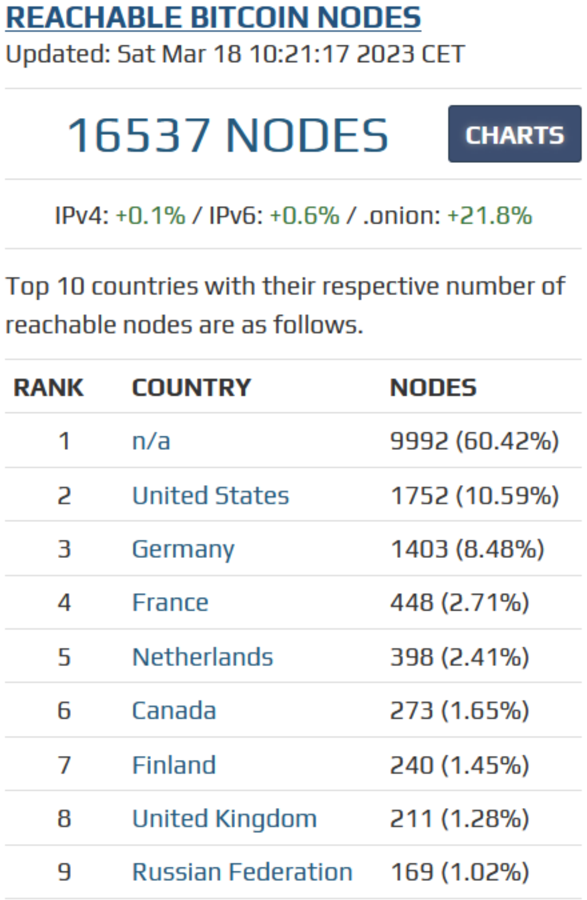


https://statoshi.info/d/000000009/unspent-transaction-output-set?orgId=1&refresh=10m&from=1483225200000&to=now

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…
- Lighting – second layer network of payment channels atop of mainnet
  - Practically instant and very low fees independently from mainnet

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



REACHABLE BITCOIN NODES

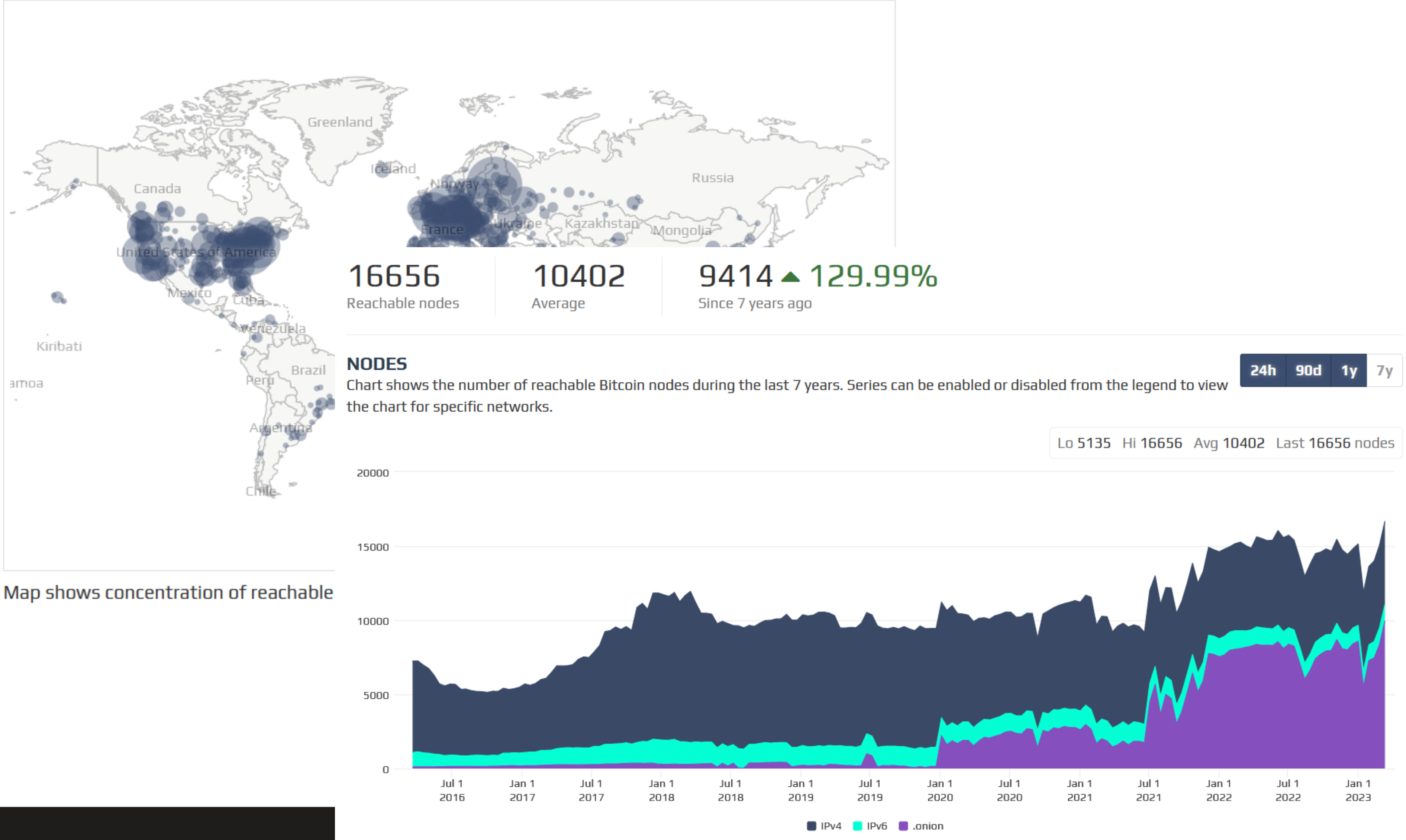
Updated: Sat Mar 18 10:21:17 2023 CET

16537 NODES CHARTS

IPv4: +0.1% / IPv6: +0.6% / .onion: +21.8%

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

RANK	COUNTRY	NODES
1	n/a	9992 (60.42%)
2	United States	1752 (10.59%)
3	Germany	1403 (8.48%)
4	France	448 (2.71%)
5	Netherlands	398 (2.41%)
6	Canada	273 (1.65%)
7	Finland	240 (1.45%)
8	United Kingdom	211 (1.28%)
9	Russian Federation	169 (1.02%)



Map shows concentration of reachable

16656 Reachable nodes

10402 Average

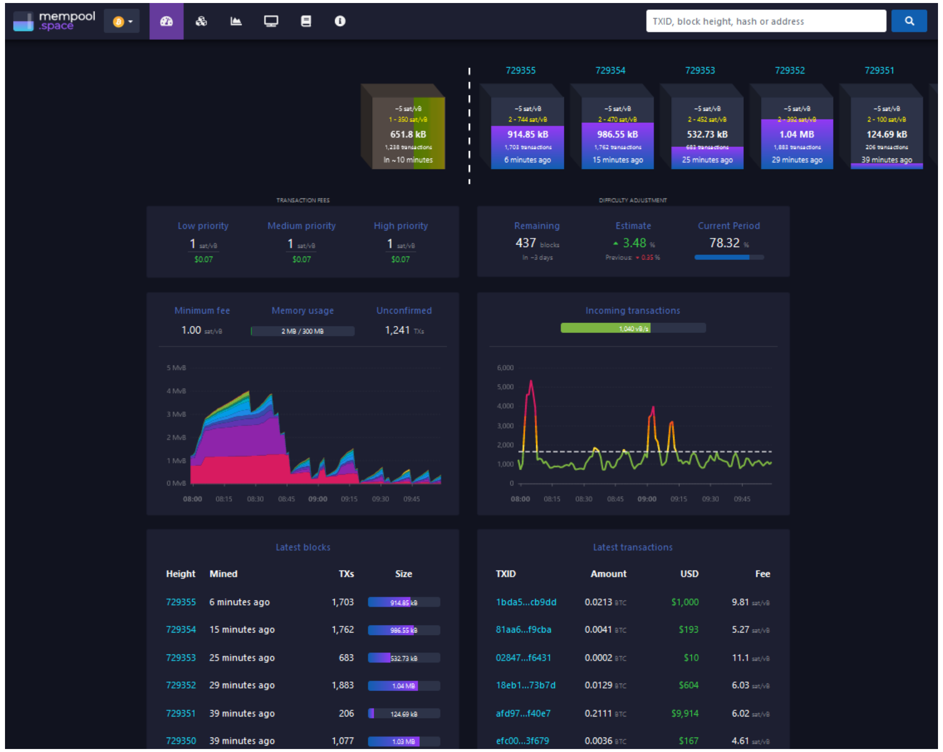
9414 ▲ 129.99% Since 7 years ago

NODES

Chart shows the number of reachable Bitcoin nodes during the last 7 years. Series can be enabled or disabled from the legend to view the chart for specific networks.

Lo 5135 Hi 16656 Avg 10402 Last 16656 nodes

Popular mempool explorer – https://mempool.space



mempool .space

TXID, block height, hash or address

	729355	729354	729353	729352	729351
~5 sat/vB	~5 sat/vB	~5 sat/vB	~5 sat/vB	~5 sat/vB	~5 sat/vB
1 - 350 sat/vB	2 - 744 sat/vB	2 - 470 sat/vB	2 - 452 sat/vB	2 - 392 sat/vB	2 - 100 sat/vB
651.8 kB	914.85 kB	986.55 kB	532.73 kB	1.04 MB	124.69 kB
1,238 transactions	1,703 transactions	1,762 transactions	683 transactions	1,883 transactions	206 transactions
In ~10 minutes	6 minutes ago	15 minutes ago	25 minutes ago	29 minutes ago	39 minutes ago

TRANSACTION FEES

Low priority	Medium priority	High priority
1 sat/vB	1 sat/vB	1 sat/vB
$0.07	$0.07	$0.07

DIFFICULTY ADJUSTMENT

Remaining	Estimate	Current Period
437 blocks	▲ 3.48 %	78.32 %
In ~3 days	Previous: ▼ 0.35 %	

Minimum fee	Memory usage	Unconfirmed
1.00 sat/vB	2 MB / 300 MB	1,241 TXs

Incoming transactions

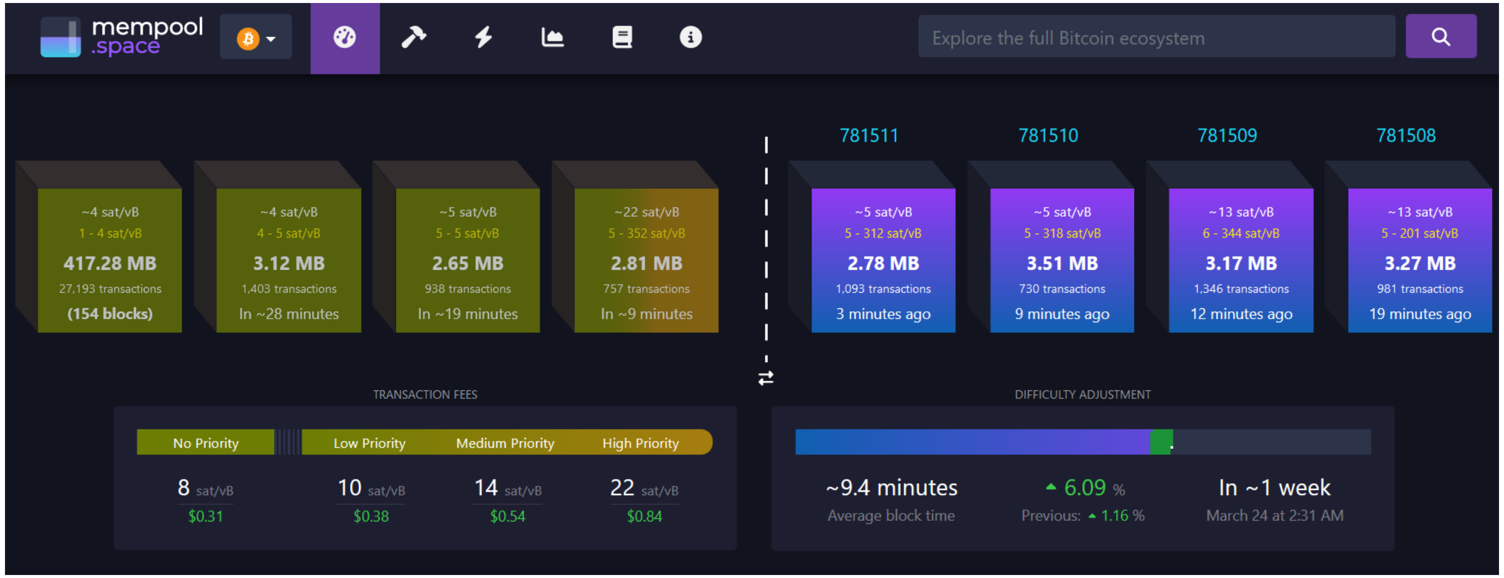
1,040 vB/s

Latest blocks

Height	Mined	TXs	Size
729355	6 minutes ago	1,703	914.85 kB
729354	15 minutes ago	1,762	986.55 kB
729353	25 minutes ago	683	532.73 kB
729352	29 minutes ago	1,883	1.04 MB
729351	39 minutes ago	206	124.69 kB
729350	39 minutes ago	1,077	1.03 MB

Latest transactions

TXID	Amount	USD	Fee
1bda5...cb9dd	0.0213 BTC	$1,000	9.81 sat/vB
81aa6...f9cba	0.0041 BTC	$193	5.27 sat/vB
02847...f6431	0.0002 BTC	$10	11.1 sat/vB
18eb1...73b7d	0.0129 BTC	$604	6.03 sat/vB
afd97...f40e7	0.2111 BTC	$9,914	6.02 sat/vB
efc00...3f679	0.0036 BTC	$167	4.61 sat/vB



mempool .space

Explore the full Bitcoin ecosystem

				781511	781510	781509	781508
~4 sat/vB	~4 sat/vB	~5 sat/vB	~22 sat/vB	~5 sat/vB	~5 sat/vB	~13 sat/vB	~13 sat/vB
1 - 4 sat/vB	4 - 5 sat/vB	5 - 5 sat/vB	5 - 352 sat/vB	5 - 312 sat/vB	5 - 318 sat/vB	6 - 344 sat/vB	5 - 201 sat/vB
417.28 MB	3.12 MB	2.65 MB	2.81 MB	2.78 MB	3.51 MB	3.17 MB	3.27 MB
27,193 transactions	1,403 transactions	938 transactions	757 transactions	1,093 transactions	730 transactions	1,346 transactions	981 transactions
(154 blocks)	In ~28 minutes	In ~19 minutes	In ~9 minutes	3 minutes ago	9 minutes ago	12 minutes ago	19 minutes ago

TRANSACTION FEES

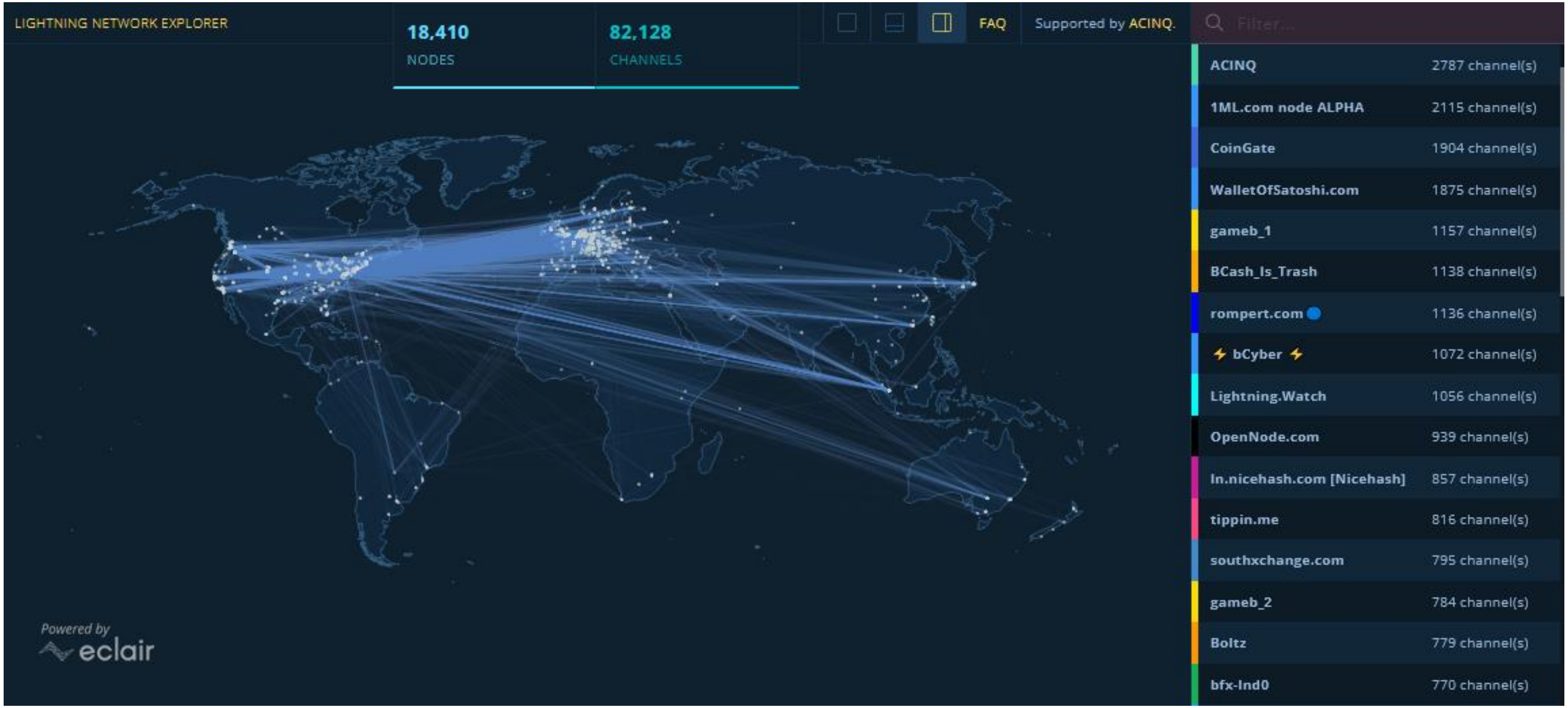
No Priority	Low Priority	Medium Priority	High Priority
8 sat/vB	10 sat/vB	14 sat/vB	22 sat/vB
$0.31	$0.38	$0.54	$0.84

DIFFICULTY ADJUSTMENT

~9.4 minutes	▲ 6.09 %	In ~1 week
Average block time	Previous: ▲ 1.16 %	March 24 at 2:31 AM

- Can be run on your own fullnode (privacy improvement)
- Testnet version https://mempool.space/testnet

Lighting network https://explorer.acinq.co/



18,410 NODES

82,128 CHANNELS

ACINQ	2787 channel(s)
1ML.com node ALPHA	2115 channel(s)
CoinGate	1904 channel(s)
WalletOfSatoshi.com	1875 channel(s)
gameb_1	1157 channel(s)
BCash_Is_Trash	1138 channel(s)
rompert.com 🔵	1136 channel(s)
⚡ bCyber ⚡	1072 channel(s)
Lightning.Watch	1056 channel(s)
OpenNode.com	939 channel(s)
ln.nicehash.com [Nicehash]	857 channel(s)
tippin.me	816 channel(s)
southxchange.com	795 channel(s)
gameb_2	784 channel(s)
Boltz	779 channel(s)
bfx-lnd0	770 channel(s)

More details

- Frequent issue – Sparrow not started with –testnet switch
- Make breakout rooms (3 people per room)
- Ask them to perform some mutual transactions
- Connect to groups and discuss:
  - Why is tx as unconfirmed? Where it is?
  - Why are we waiting some minutes?
  - How to cheat on someone who will sell us car right after tx is in mempool?
    - double spent with higher fee => Invalidation of original tx
    - Doublespent tx can be prepared into file as binary blob
    - If already mined, it is more difficult, but still somewhat possible (chain reorg)

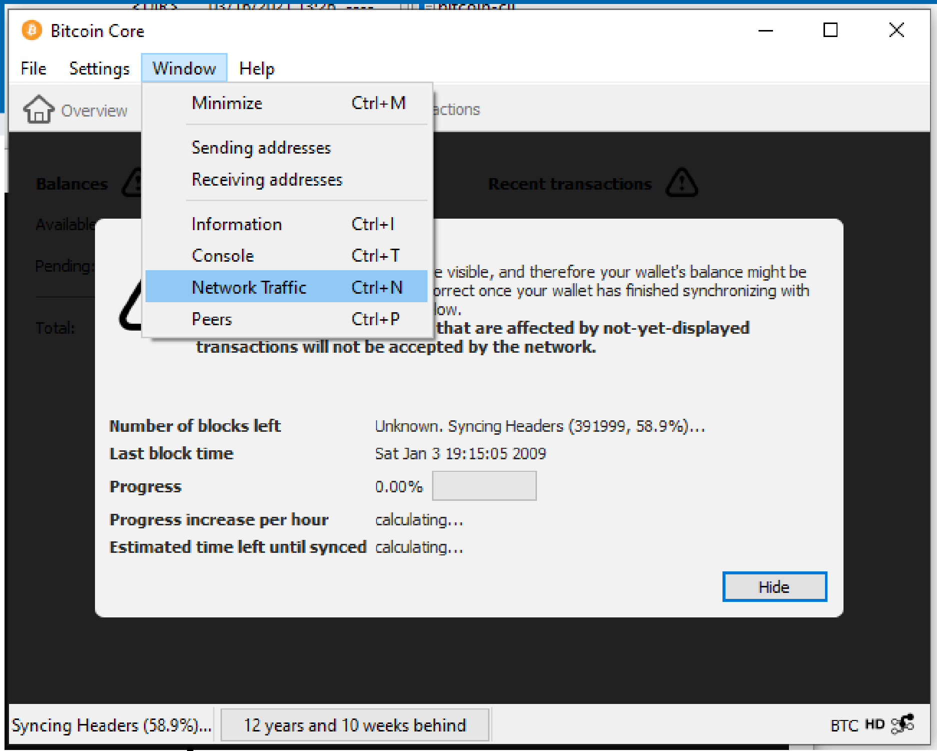
INTRO

TASK: USING BITCOIN CORE

More details

- Ask people to run GUI, see the connected nodes, locate block files
- Explain how “Chancellor … “ got there (coinbase data, used to randomize block during mining, pool info…)
- 100 blocks / file
- Importance of small blockchain => more fullnodes possible to be run => better decentralization

Own work: Using API of full node



e visible, and therefore your wallet's balance might be
orrect once your wallet has finished synchronizing with
low.
that are affected by not-yet-displayed transactions will not be accepted by the network.

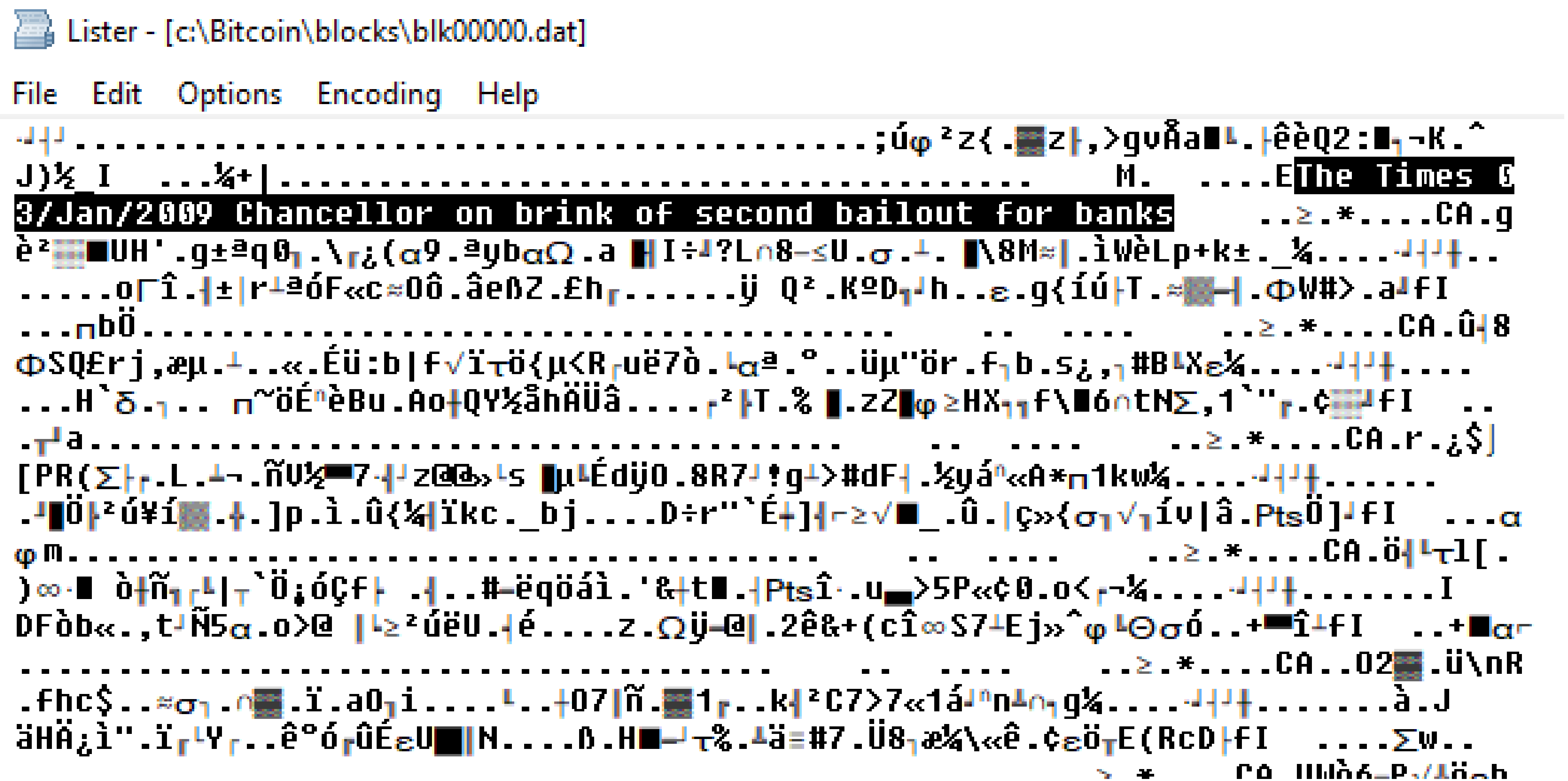
Number of blocks left Unknown. Syncing Headers (391999, 58.9%)...
Last block time Sat Jan 3 19:15:05 2009
Progress 0.00%
Progress increase per hour calculating...
Estimated time left until synced calculating...

Syncing Headers (58.9%)...
12 years and 10 weeks behind

- 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?



```
-┘┤┘.................................;úφ²z{.▓z├,>gvÅa█└.├êèQ2:█┐¬K.^
J)½_I  ...¼+|.......................   M.  ....EThe Times 0
3/Jan/2009 Chancellor on brink of second bailout for banks   ..≥.*....CA.g
è²▒■UH'.g±ªq0┐.\┌¿(α9.ªybαΩ.a ▐I÷┘?L∩8─≤U.σ.┴. ▐\8M≈|.ìWèLp+k±._¼....┘┤┘╪..
.....oΓî.┤±|r┴ªóF«c≈0ô.âeßZ.£h┌......ÿ Q².KºD┐┘h..ε.g{íú├T.≈▓─|.ΦW#>.a┘fI
...┌bÖ.........................   ..  ....   ..≥.*....CA.û┤8
ΦSQ£rj,æµ.┴..«.Éü:b|f√ïτö{µ<R┌uë7ò.└αª.°..üµ"ör.f┐b.s¿,┐#B└Xε¼....┘┤┘╪....
...H`δ.┐.. ⊓~öÉⁿèBu.Ao╪QY½åhÄÜâ....┌²├T.% ▐.zZ▐φ≥HX┐┐f\█6∩tNΣ,1`"┌.¢▒┘fI  ..
.┬┘a...........................   ..  ....   ..≥.*....CA.r.¿$|
[PR(Σ├┌.L.┴¬.ñU½▀7┤┘z@@»└s ▐µ└Édÿ0.8R7┘!g┴>#dF┤.½yáⁿ«A*⊓1kw¼....┘┤┘╪......
.┘▐Ö├²ú¥í▒.╪.]p.ì.û{¼|ïkc._bj....D÷r"`É╪]┤⌐≥√■_.û.|ç»{σ┐√┐íυ|â.₧sÖ]┘fI  ...α
φm.............................   ..  ....   ..≥.*....CA.ö┤└τl[.
)∞·■ ò╪ñ┐┌└|┬`Ö¡óÇf├ .┤..#─ëqöáì.'&╪t█.┤₧sî·.u▄>5P«¢0.o<┌¬¼....┘┤┘╪........I
DFòb«.,t┘Ñ5α.o>@ |└≥²úëU.┤é....z.Ωÿ─@|.2ê&+(cî∞S7┴Ej»^φ└Θσó..+▀î┴fI  ..+■α⌐
...............................   ..  ....   ..≥.*....CA..02▓.Ü\nR
.fhc$..≈σ┐.∩▓.ï.a0┐i....└..╪07|ñ.▓1┌..k┤²C7>7«1á┘ⁿn┴∩┐g¼....┘┤┘╪........à.J
äHÄ¿ì".ï┌└Y┌..ê°ó┌ÛÉεU█|N....ß.H■─┘τ%.┴ä≡#7.Ü8┐æ¼\«ê.¢εö┬E(RcD├fI  ....Σw..
```

Run strings on already downloaded blocks

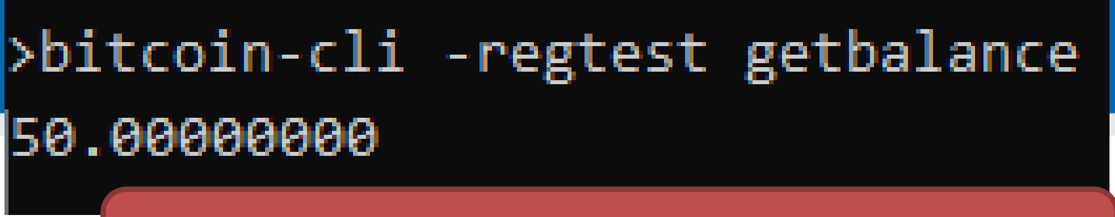
- **`strings`** command on Linux
- **`strings`** on Windows: https://docs.microsoft.com/en-us/sysinternals/downloads/strings
- `c:\Bitcoin\blocks>strings -n 20 *.dat`

TASK: USING BITCOIN-CLI (REGTEST)

More details

- Check before seminar the commands (frequent change of API)
  - 0.21.0 requires min fee etc (**`settxfee 0.00002`**)
- Explain why **`generatetoaddress`** 101
  - Consensus rule: coinbase can be spent only after 100 blocks => less motivation for miners to fiddle with chain reorg
- Explain halving (210000 blocks on mainnet, 150 on regtest)
- Explain why after sending 10 to other, resulting balance is 49.999…
  - Mining fee subtracted (but we are miners! But we will get fee only in 100 blocks)

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

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 transaction 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

SINGLE-SIGNATURE WALLET (SW-ONLY)

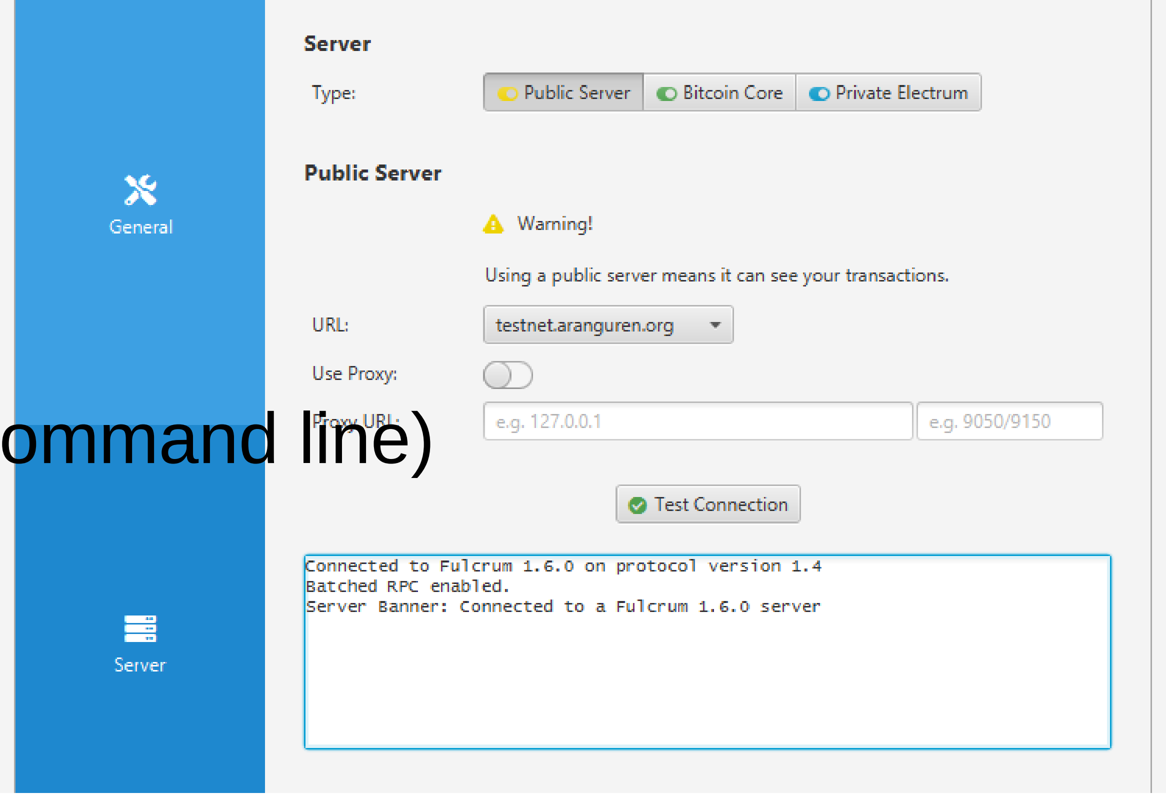
Sparrow wallet (v1.6.6)

- https://www.sparrowwallet.com/download/
- For serious work, always verify binary releases (`gpg --verify`)
- Well-known and maintained, Java-based, minimum other dependencies, focus on medium and advanced users
- Sparrow is “signing coordinator” – private keys can inside or elsewhere
- Basic functionality
  - Open-source wallet, non-custodial wallet
  - Support for software and hardware wallets, multisignature coordinator
  - Whirlpool CoinJoin client
  - Supports also advanced features (PayJoin, Taproot addresses…)

(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)



Server

Type: Public Server

Public Server

⚠ Warning!

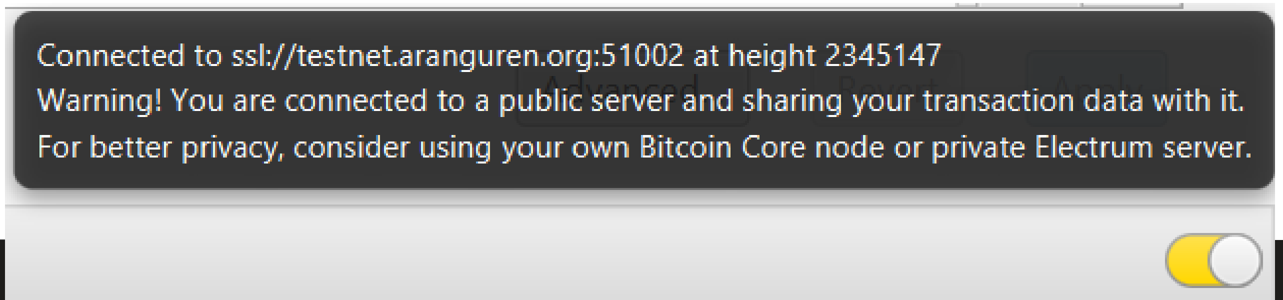
Using a public server means it can see your transactions.

URL: testnet.aranguren.org

Use Proxy: ○

Proxy URL: e.g. 127.0.0.1 e.g. 9050/9150

```
Connected to Fulcrum 1.6.0 on protocol version 1.4
Batched RPC enabled.
Server Banner: Connected to a Fulcrum 1.6.0 server
```



Connected to ssl://testnet.aranguren.org:51002 at height 2345147
Warning! You are connected to a public server and sharing your transaction data with it.
For better privacy, consider using your own Bitcoin Core node or private Electrum server.

Generating new “wallet”

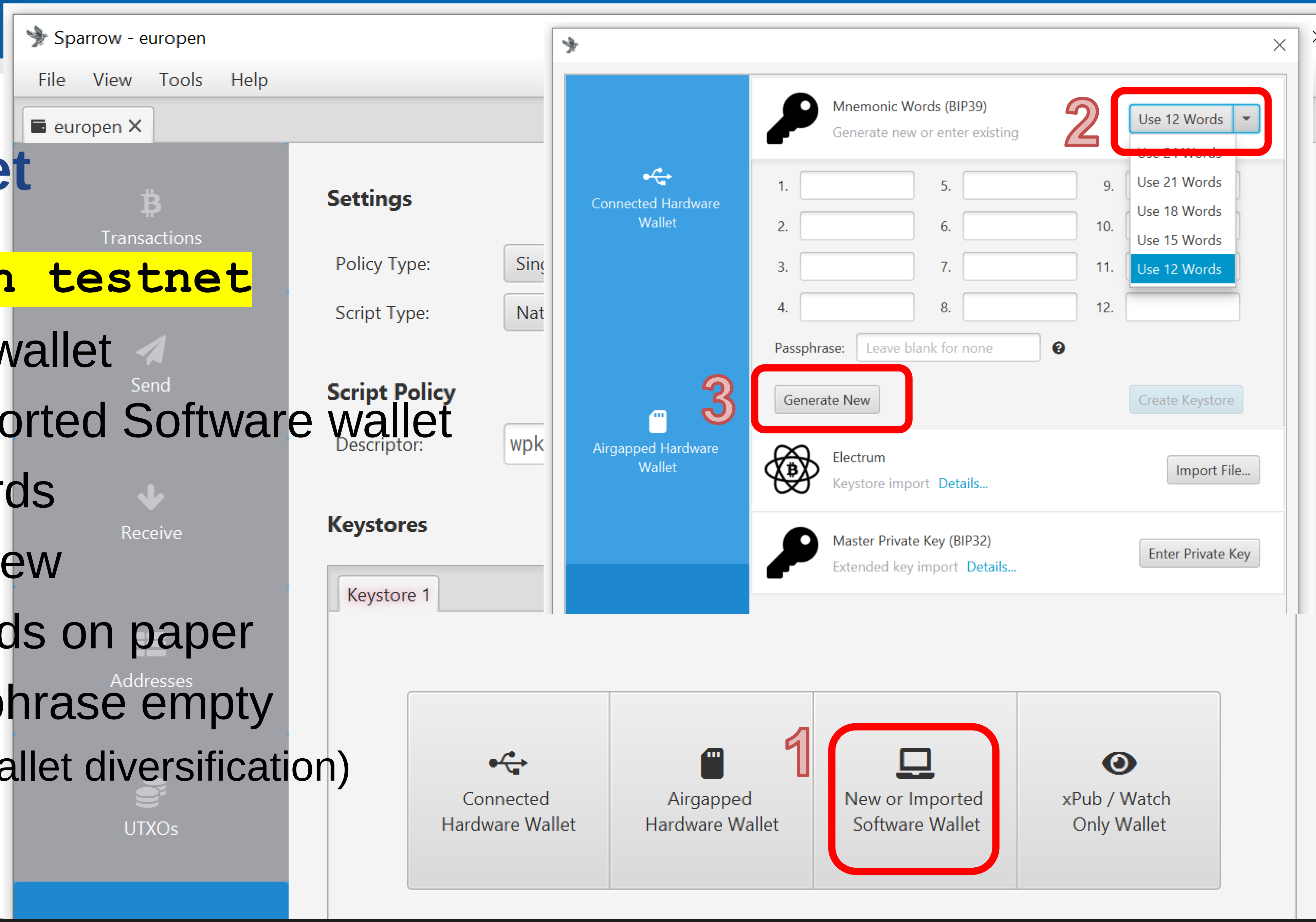
- A “wallet” is key management software controlling your private and public keys (ECDSA, Schnorr)
- The most important part of wallet is random number called root seed (128 or 256 bits)
- Root seed is used to deterministically generate practically unlimited number of keypairs
  - Specified in BIP32, “root seed” and “derivation path” used to derive next private key => next public key => next address
- Clever construction allowing to compute future public keys (and only public keys) for specified derivation path without the need for root seed (aka xpub or extended public key)
  - Knowledge of xpub allows to compute all future public keys, but not private keys
  - Owner of root seed can compute all future private keys and their corresponding public keys
  - xpub allows to pay someone to fresh addresses noninteractively (no interaction with owner of root seed required), receiver will only later compute candidate private keys and their public keys to check for total balance (== set of UTXOs)
- Wallet software is monitoring blockchain for addresses corresponding to stored root seed (or xpub)
- Root seed can be stored:
  1. Directly in software wallet (file on harddisk, optionally encrypted) == aka hot wallet, least secure against malware
  2. Loaded every time before use (e.g., from QR code), still vulnerable to malware during use
  3. On external hardware signing device called hardware wallet (the most secure option)

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)



Policy Type: Sing

Script Type: Nat

Descriptor: wpk

Mnemonic Words (BIP39)
Generate new or enter existing

1. 2. 3. 4. 5. 6. 7. 8. 9. 10. 11. 12.

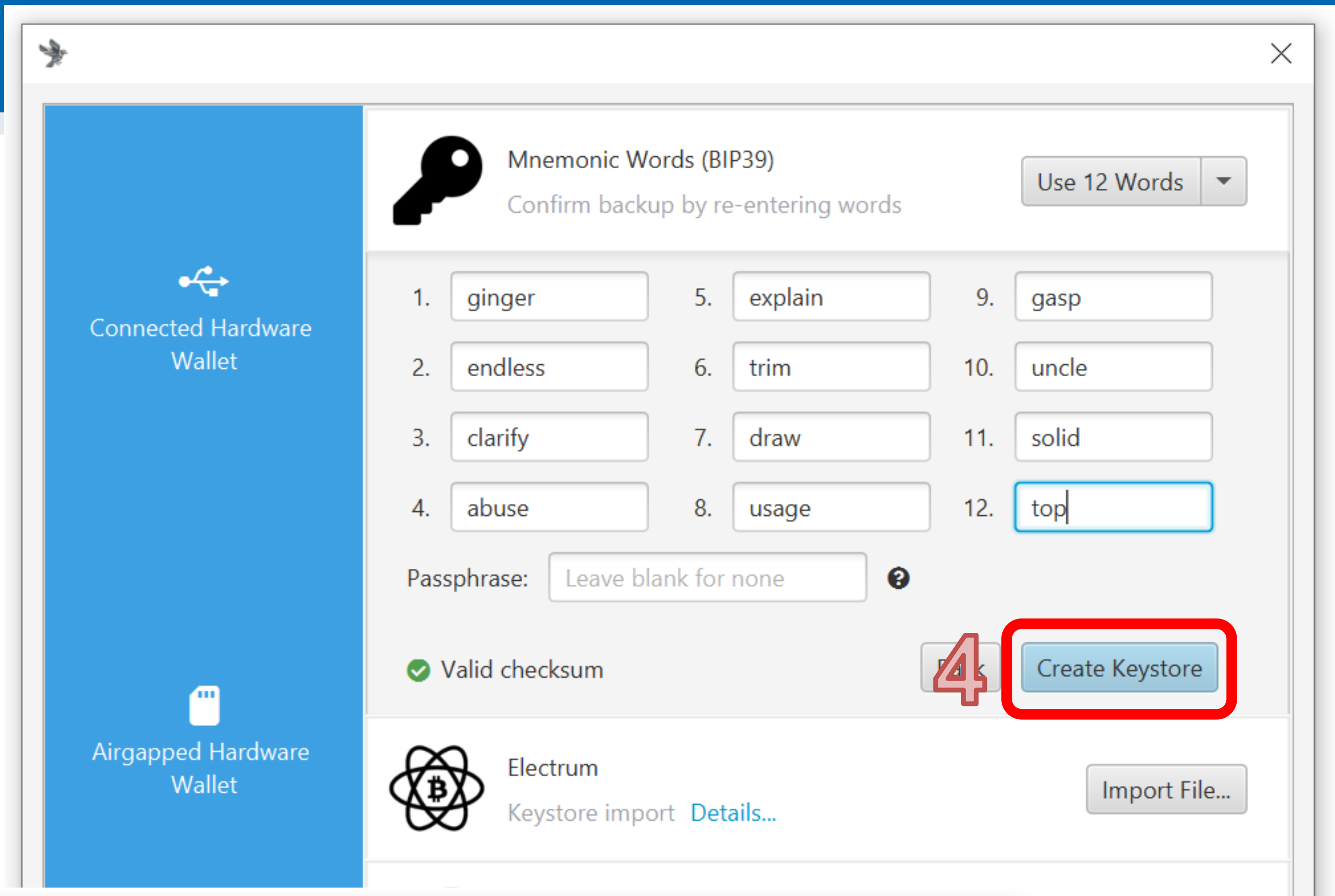
Passphrase: Leave blank for none

Electrum
Keystore import Details...

Master Private Key (BIP32)
Extended key import Details...

Create wallet

4. Create Keystore
- Confirm backup
- Reenter words
5. Import Keystore



Mnemonic Words (BIP39)

Confirm backup by re-entering words

Use 12 Words

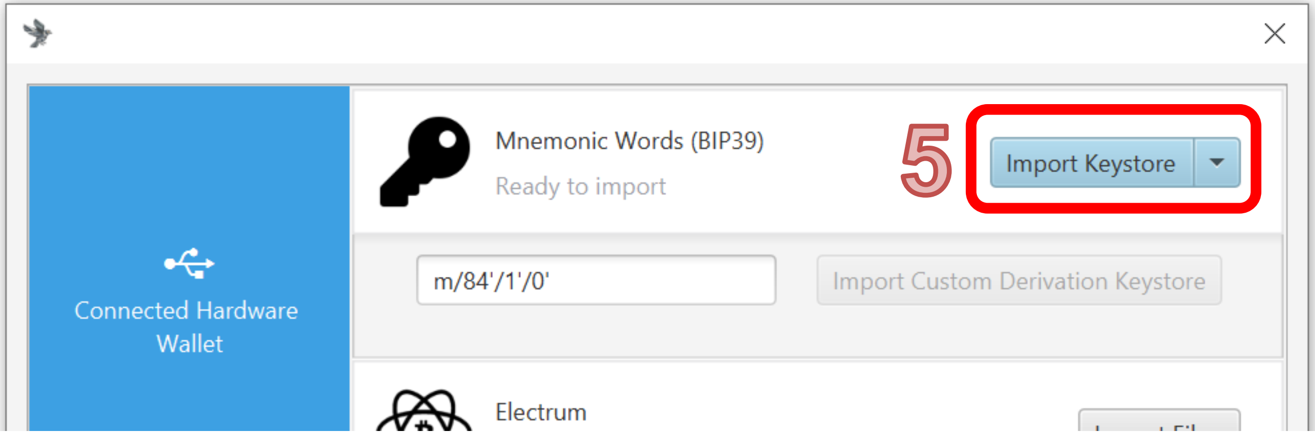
1.	ginger	5.	explain	9.	gasp
2.	endless	6.	trim	10.	uncle
3.	clarify	7.	draw	11.	solid
4.	abuse	8.	usage	12.	top

Passphrase: Leave blank for none

✓ Valid checksum

Connected Hardware Wallet
Airgapped Hardware Wallet
4
Create Keystore
Electrum
Keystore import Details...
Import File...

Enter Private Key



Mnemonic Words (BIP39)

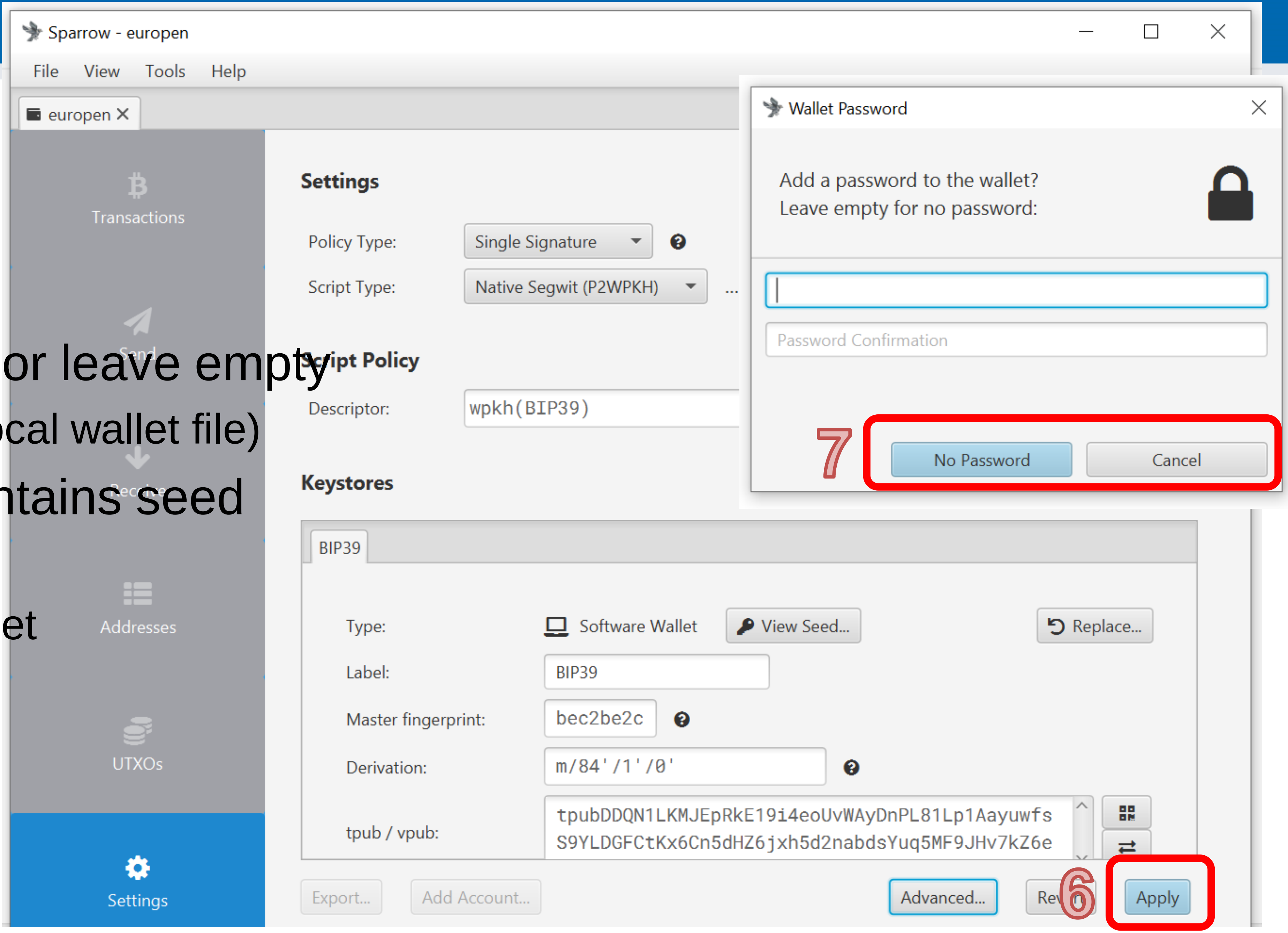
Ready to import

m/84'/1'/0'

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



Sparrow - europen

Wallet Password

Add a password to the wallet?
Leave empty for no password:

Settings

Policy Type: Single Signature

Script Type: Native Segwit (P2WPKH)

Script Policy

Descriptor: wpkh(BIP39)

Keystores

BIP39

Type: Software Wallet

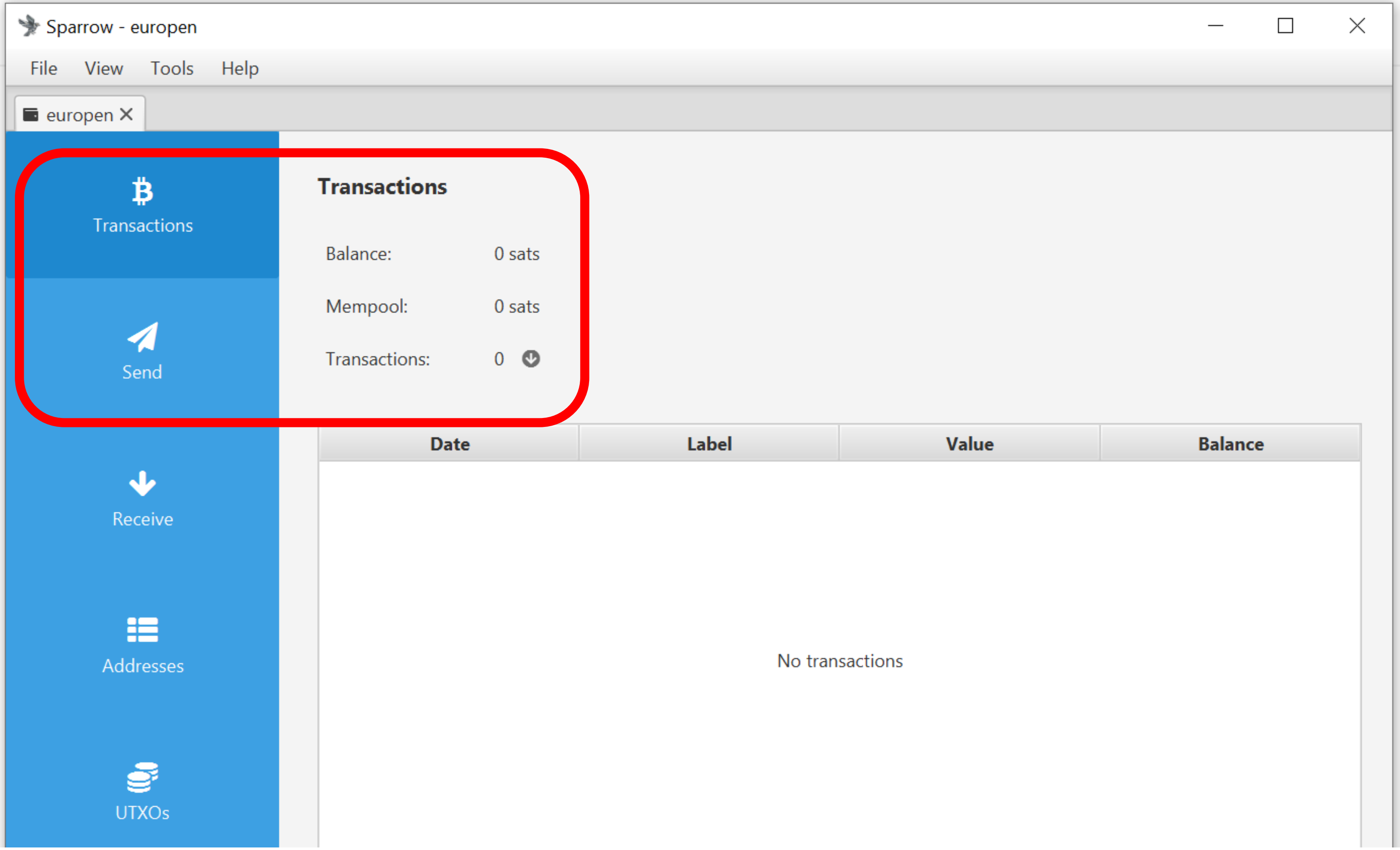
Label: BIP39

Master fingerprint: bec2be2c

Derivation: m/84'/1'/0'

tpub / vpub: tpubDDQN1LKMJEpRkE19i4eoUvWAyDnPL81Lp1AayuwfsS9YLDGFCtKx6Cn5dHZ6jxh5d2nabdsYuq5MF9JHv7kZ6e

Wallet created (but empty ☺)



Transactions

Balance: 0 sats

Mempool: 0 sats

Transactions: 0

Date	Label	Value	Balance

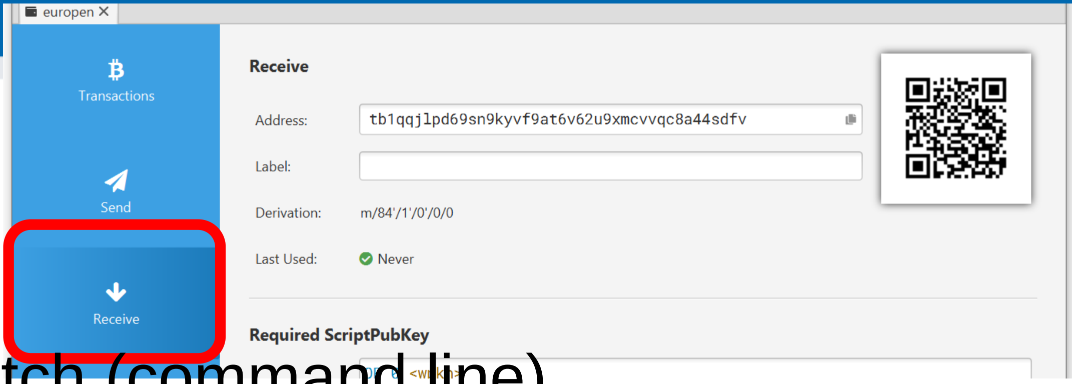
No transactions

Receiving (testnet) bitcoins

- You generate new “address”
  - deterministically derived from your root seed and fresh derivation path (path + counter) => new ECDSA keypair [BIP32]
  - public key X is pasted into locking script (“who can sign with private key verifiable with X can move bitcoin further”) and hashed => “address” [P2SH/P2WSH] (Pay to witness script hash)
- Service coinfaucet.eu owns multiple tBTC
  - Service is providing limited number of test bitcoins (tBTC) for free
  - Service owns UTXOs => someone previously locked some tBTC to their keypair(s)
  - Service creates new transaction with some tBTC locked to your “address”
  - New transaction is broadcasted to Bitcoin P2P network and stored in mempools (set of unconfirmed transactions)
- Miners will eventually include this transaction into new block (head of blockchain)
  - Confirmed and removed from mempools
  - Your Sparrow wallet is monitoring both mempool and blockchain (instant notification about pending transaction)

Getting test bitcoins (tBTC)

1



Receive

Address: tb1qqjlpd69sn9kyvf9at6v62u9xmcvvqc8a44sdfv

Label:

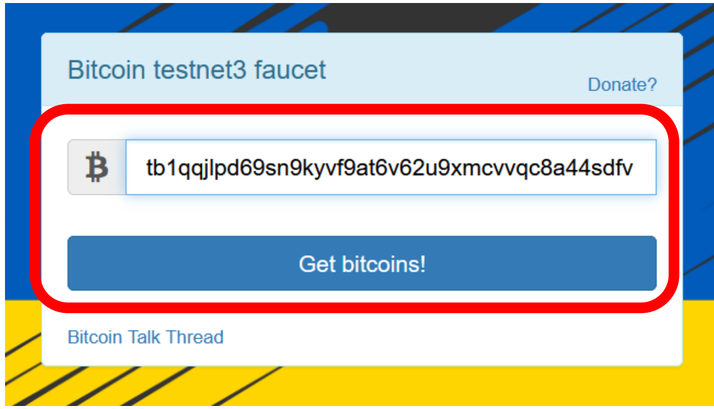
Derivation: m/84'/1'/0'/0/0

Last Used: ✓ Never

Required ScriptPubKey

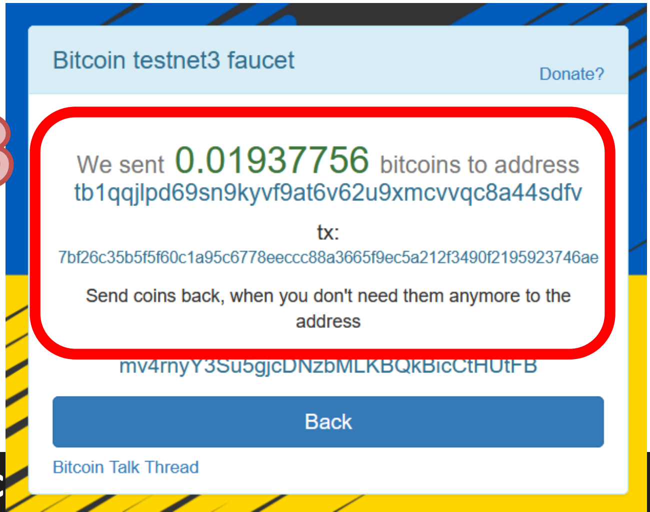
- If not running, run your wallet with testnet switch (command line)
  - E.g., `./sparrow -n testnet`
  - Generate new (testnet) receive address
- Go to https://coinfaucet.eu/en/btc-testnet/
  - If doesn't work use https://testnet-faucet.com/btc-testnet/
  - Insert your testnet receive address
  - You 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



₿ tb1qqjlpd69sn9kyvf9at6v62u9xmcvvqc8a44sdfv

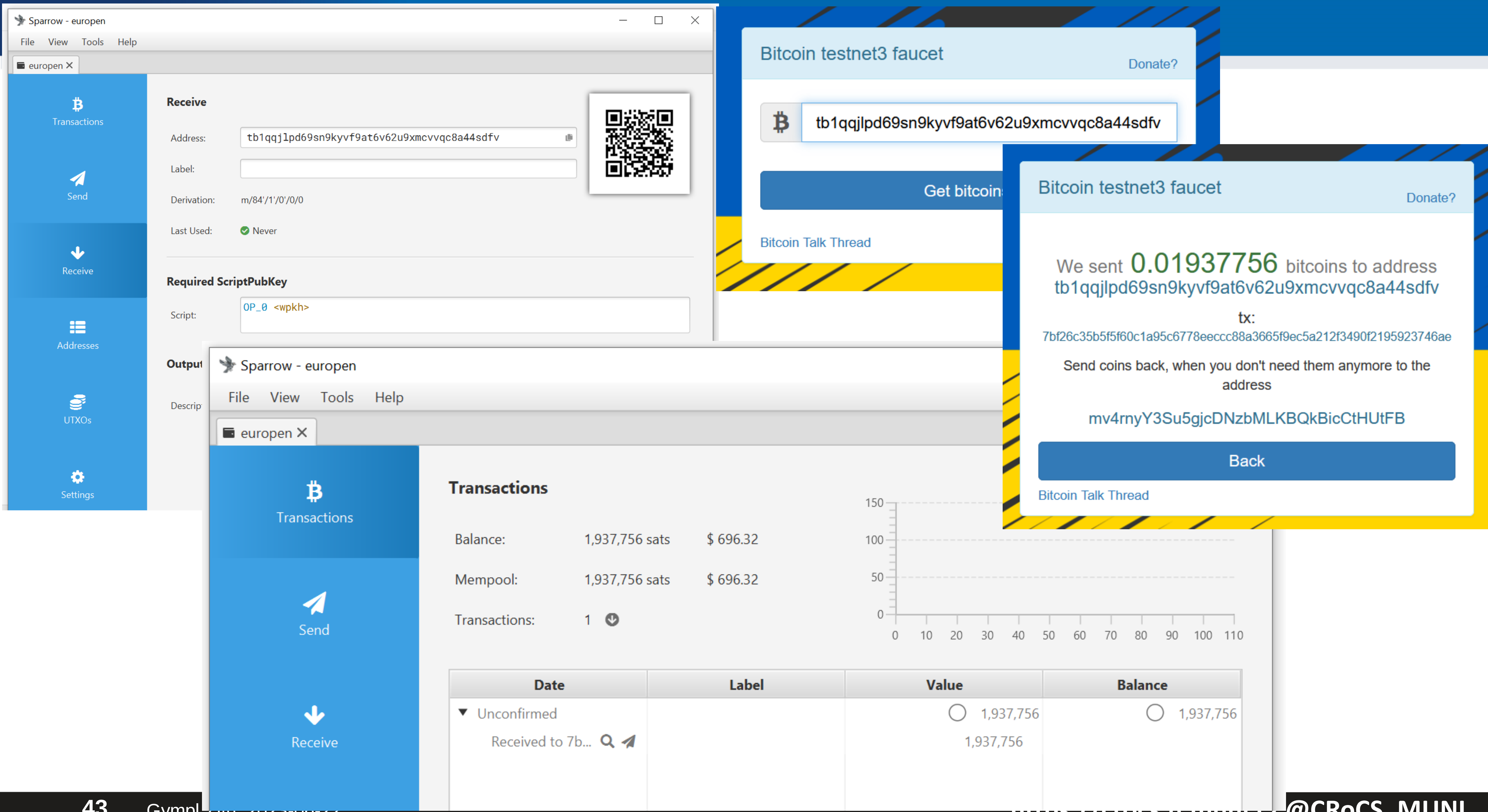
3



We sent 0.01937756 bitcoins to address tb1qqjlpd69sn9kyvf9at6v62u9xmcvvqc8a44sdfv

tx: 7bf26c35b5f5f60c1a95c6778eeccc88a3665f9ec5a212f3490f2195923746ae

Send coins back, when you don't need them anymore to the address mv4rnyY3Su5gjcDNzbMLKBQkBicCtHUtFB



Sparrow - europen

Receive

Address: tb1qqj1pd69sn9kyvf9at6v62u9xmcvvqc8a44sdfv

Label:

Derivation: m/84'/1'/0'/0/0

Last Used: Never

Required ScriptPubKey

Script: OP_0 <wpkh>

Output

Descrip

Bitcoin testnet3 faucet

tb1qqjlpd69sn9kyvf9at6v62u9xmcvvqc8a44sdfv

Bitcoin testnet3 faucet

We sent 0.01937756 bitcoins to address tb1qqjlpd69sn9kyvf9at6v62u9xmcvvqc8a44sdfv

tx:
7bf26c35b5f5f60c1a95c6778eeccc88a3665f9ec5a212f3490f2195923746ae

Send coins back, when you don't need them anymore to the address

mv4rnyY3Su5gjcDNzbMLKBQkBicCtHUtFB

Sparrow - europen

Transactions

Balance: 1,937,756 sats $ 696.32

Mempool: 1,937,756 sats $ 696.32

Transactions: 1

Date	Label	Value	Balance
▼ Unconfirmed		○ 1,937,756	○ 1,937,756
Received to 7b...		1,937,756	

Blockchain explorers

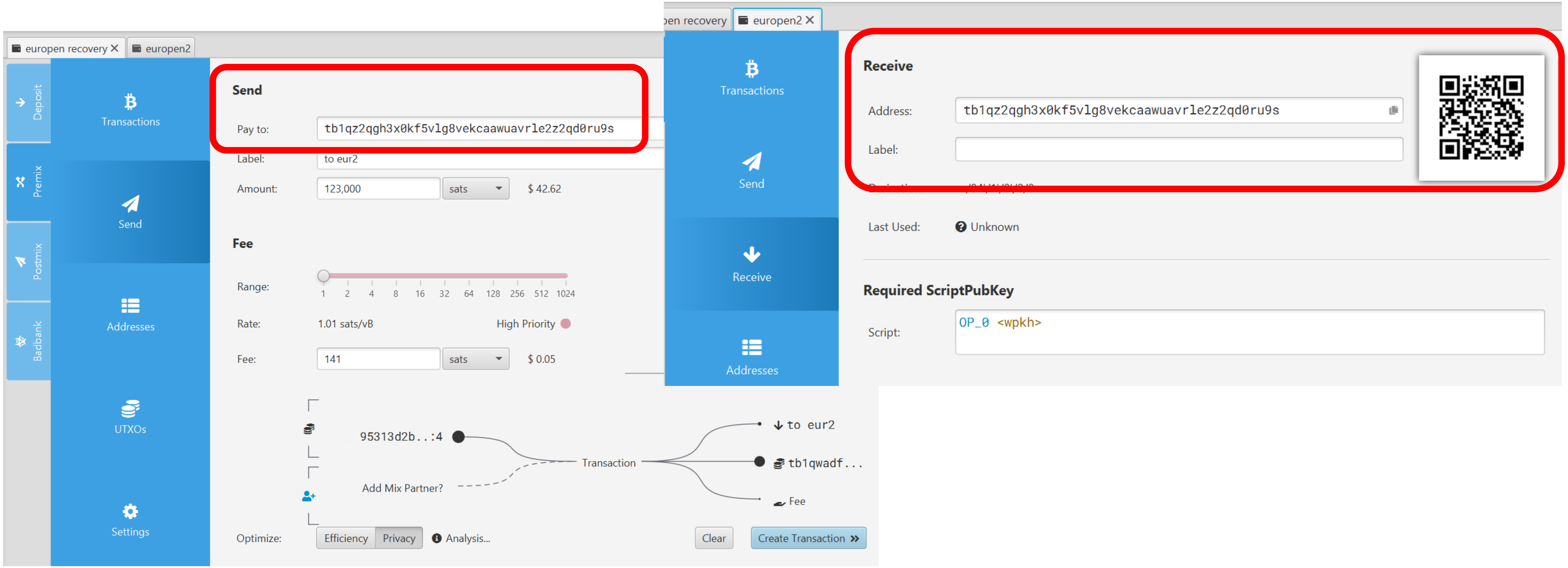
- Everybody with access to Bitcoin P2P network can analyze blockchain
  - Everybody running Bitcoin fullnode
  - All past transactions, human-readable visualizations, search for address…
  - Convenient quick check of funds send
- Third parties are operating public explorers (convenient, but privacy)
  - It is very important to use Tor Browser when accessing public block explorers
  - Explorer operator may log your IP address and transactions you are searching for and later sell it (chain surveillance companies)
    - Heuristic assumption that you are the owner of funds for searched transaction
- Ideally use your own full node with your own blockchain explorer
- Sparrow wallet allows you to visualize your transactions
  - Inputs, outputs, feed paid

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



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

Optimize: Efficiency Privacy

Receive

Address: tb1qz2qgh3x0kf5vlg8vekcaawuavrle2z2qd0ru9s

Label:

Derivation: m/84'/1'/0'/0/0

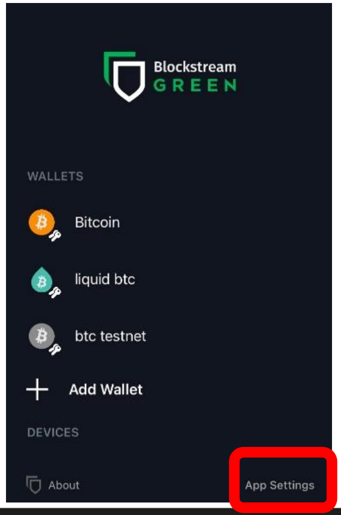
Last Used: Unknown

Required ScriptPubKey

Script: OP_0 <wpkh>

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



Blockstream GREEN

WALLETS

Bitcoin

liquid btc

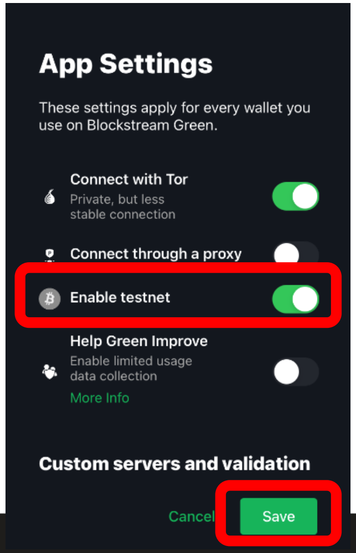
btc testnet

Add Wallet

DEVICES

About

App Settings



App Settings

These settings apply for every wallet you use on Blockstream Green.

Connect with Tor
Private, but less stable connection

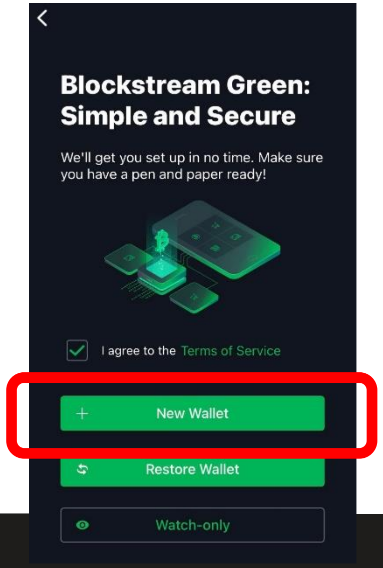
Connect through a proxy

Enable testnet

Help Green Improve
Enable limited usage data collection
More Info

Custom servers and validation

Cancel Save



Blockstream Green: Simple and Secure

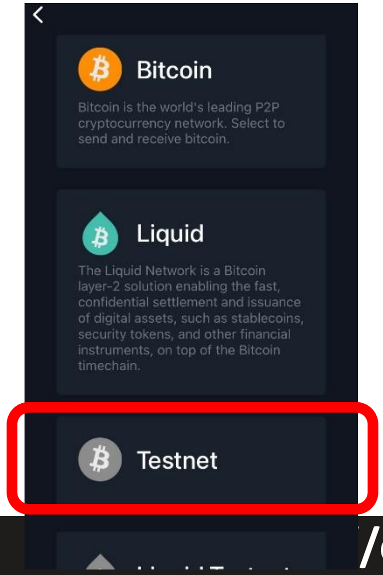
We'll get you set up in no time. Make sure you have a pen and paper ready!

☑ I agree to the Terms of Service

New Wallet

Restore Wallet

Watch-only



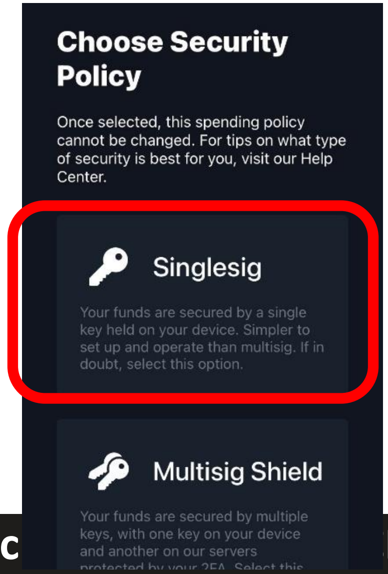
Bitcoin

Bitcoin is the world's leading P2P cryptocurrency network. Select to send and receive bitcoin.

Liquid

The Liquid Network is a Bitcoin layer-2 solution enabling the fast, confidential settlement and issuance of digital assets, such as stablecoins, security tokens, and other financial instruments, on top of the Bitcoin timechain.

Testnet



Choose Security Policy

Once selected, this spending policy cannot be changed. For tips on what type of security is best for you, visit our Help Center.

Singlesig

Your funds are secured by a single key held on your device. Simpler to set up and operate than multisig. If in doubt, select this option.

Multisig Shield

Your funds are secured by multiple keys, with one key on your device and another on our servers protected by your 2FA. Select this

Questions

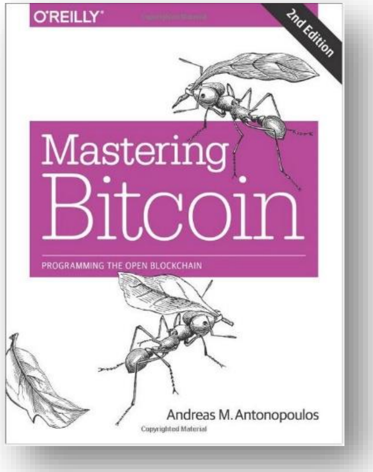
- Can you get less than 1 bitcoin?
- How can you get some real bitcoin(s)? (three different options)
- How can I pay you 1btc if I have only one UTXO worth of 5btc?
- Can you reverse bitcoin payment if send to wrong address?
- Why “Not your keys, not your bitcoin”? What is non-custodial wallet?
- How 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?
- If I will send you bitcoin on-chain, can you tell from whom I got it?
- Why should you use fresh new address for every receive transaction?
- Why is theoretical maximal limit of on-chain transactions ~6-7tx/sec?
- 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?

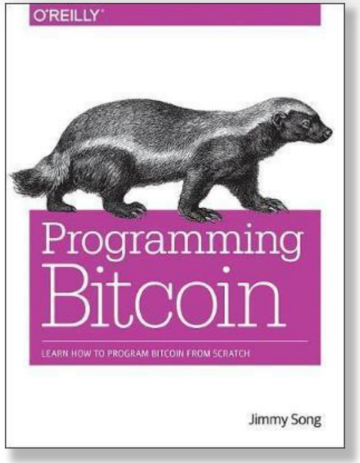
(Look for your testnet txs from bitcoin core client)

- 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`**

Further reading

- Mastering Bitcoin (Andreas M. Antonopoulos and others)
  - https://github.com/bitcoinbook/bitcoinbook
- Programming Bitcoin (Jimmy Song)
  - https://github.com/jimmysong/programmingbitcoin
- List of interesting resources
  - https://blockonomi.com/bitcoin-educational-resources/
  - https://learnmeabitcoin.com/, https://learnmeabitcoin.com/technical/
- Bitcoin Twitter, Nostr (https://nostr.com/clients)

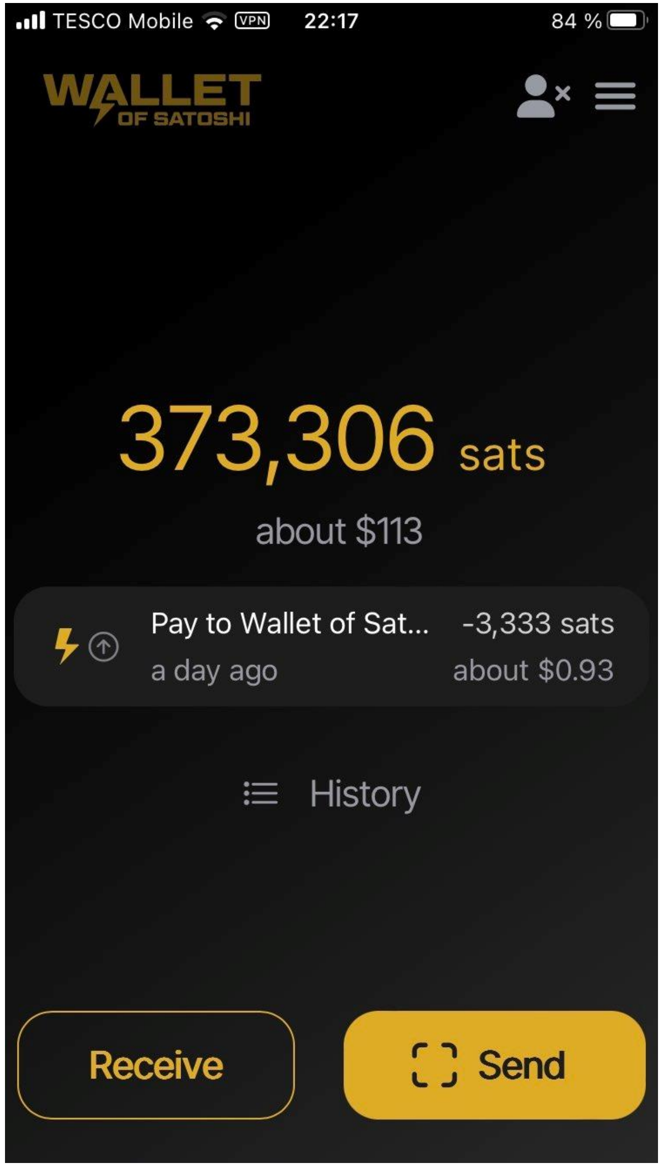




Getting some real sats (1/100000000 ₿)

- You can get/buy fraction of bitcoin
- Transaction on mainnet
  – potentially costly, ~10mins to execute
  – Mainnet is not for buying coffee
- Satoshies on Lighting – instant and near free

1. Download Wallet of Satoshi
2. Click Receive → QRCode displayed
3. Come to get some
4. Try and learn



373,306 sats
about $113

Pay to Wallet of Sat... -3,333 sats
a day ago about $0.93