EUROPEN 2022 TUTORIAL
Tutoriál: “Praktické využití prahové kryptografie (Multisig) a anonymizačních technik (CoinJoin) v Bitcoinu i mimo něj”

Bitcoin backup, multisig and CoinJoin, version 0.91

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

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

CROCS
Centre for Research on Cryptography and Security

Top questions (1)

Anonymous 0

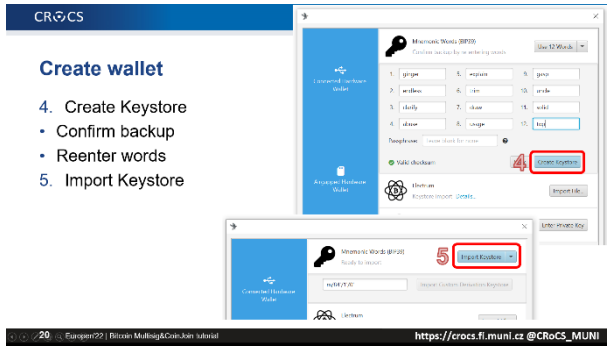
I think that Proof of Steak (PoS) is better than Proof of Water (PoW) - change my mind!

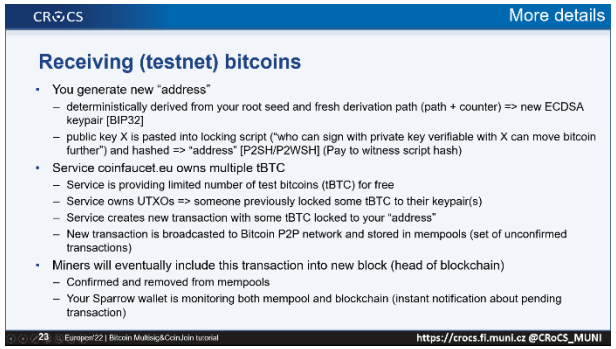
- Raise your hand if stuck, we will help you
- Use slido.com with code #europen22 for longer questions
  - We will check occasionally and try to answer

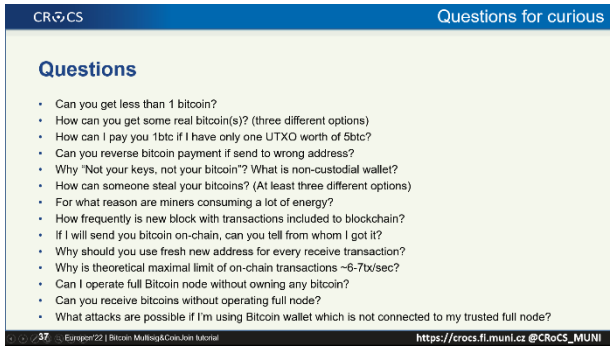
Join at
slido.com
#europen22

Types of slides (only in presentation, not in print)

- White background – standard slide with instructions
- Blue background – additional information
- Green background – questions for curious reader







slido

Audience Q&A Session

ⓘ Start presenting to display the audience questions on this slide.

WHY BITCOIN?

Especially if you are not interested in Bitcoin.

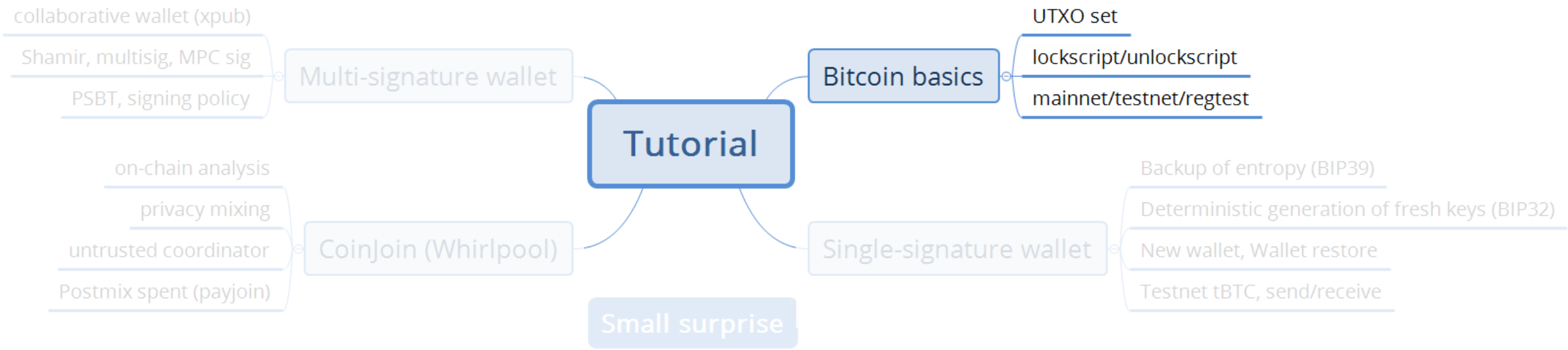
https://twitter.com/DominicFrisby/status/1388448025970884609

Goals for this tutorial

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

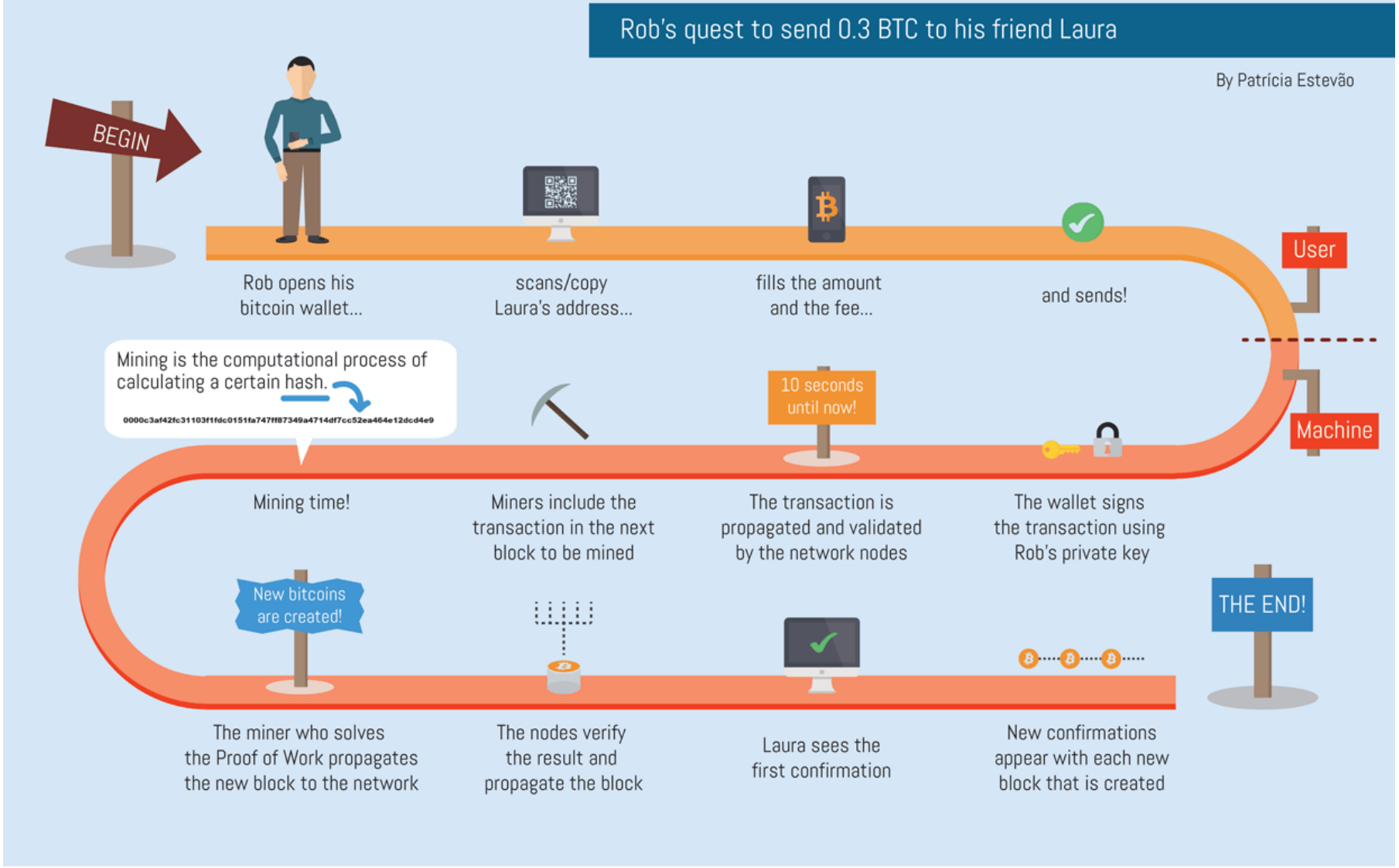
- Bitcoin does not fix everything, but is on frontline
  - No safety net, no chargeback, attacker anonymous => security technique must really work, great for battle-testing security ideas, natural “bug bounty program”
- 5 main tech pieces we will cover (also usable outside Bitcoin world)
  1. How to 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 broadcast, mpc sig)
  4. How to introduce restricted signing policy (time, limit… lockscript/multisig)
  5. How to protect your financial privacy (CoinJoin, Tor)

Goals for this tutorial

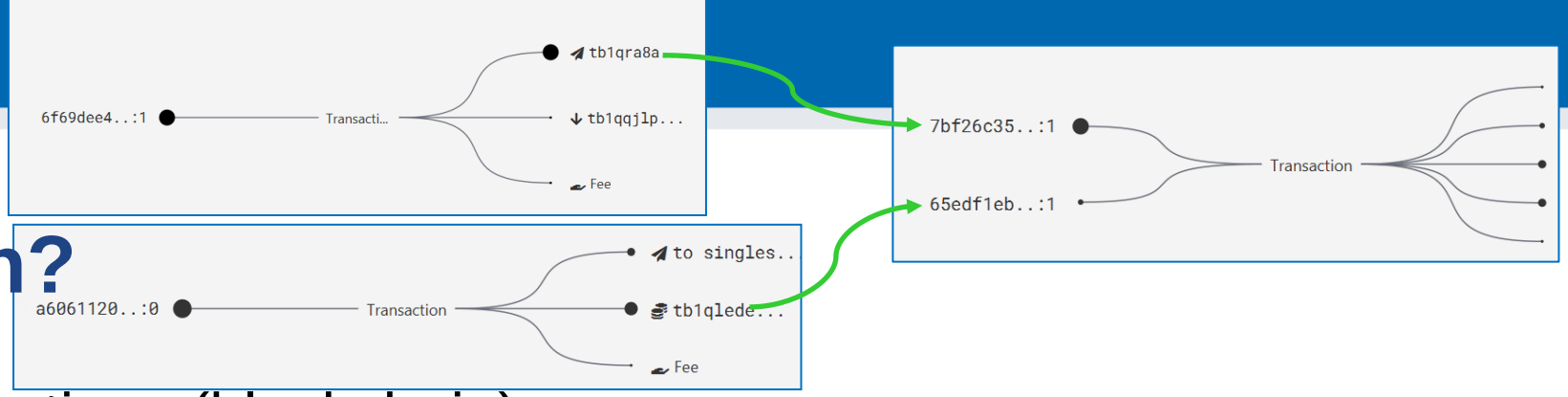


BASICS

THE BITCOIN TRANSACTION LIFE CYCLE



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



Where is my bitcoin?

- 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!

Sparrow wallet (v1.6.5)

- 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
- 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…)

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/

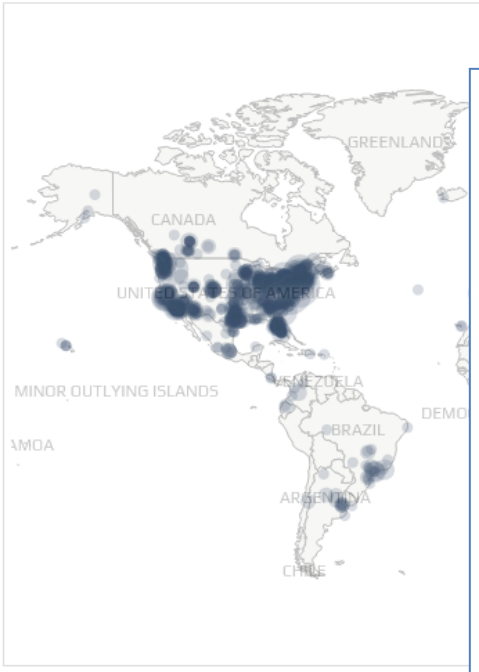
REACHABLE BITCOIN NODES
Updated: Thu Mar 24 09:37:20 2022 CET

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.

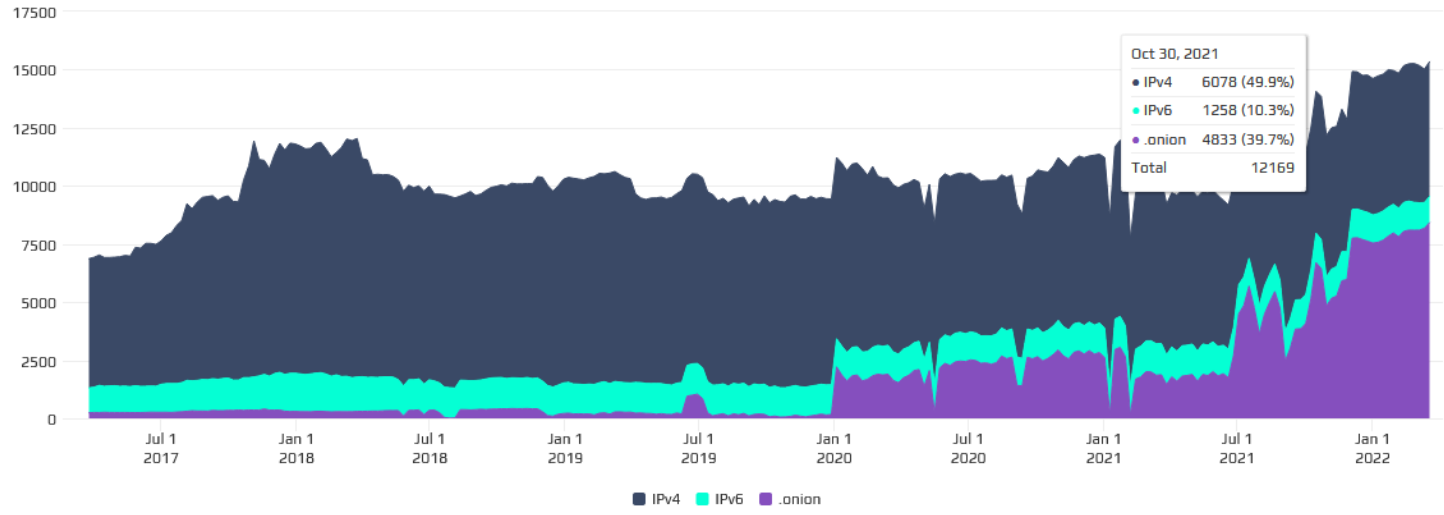
15340	10451	8472 ▲ 123.35%
Reachable nodes	Average	Since 1825 days ago

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



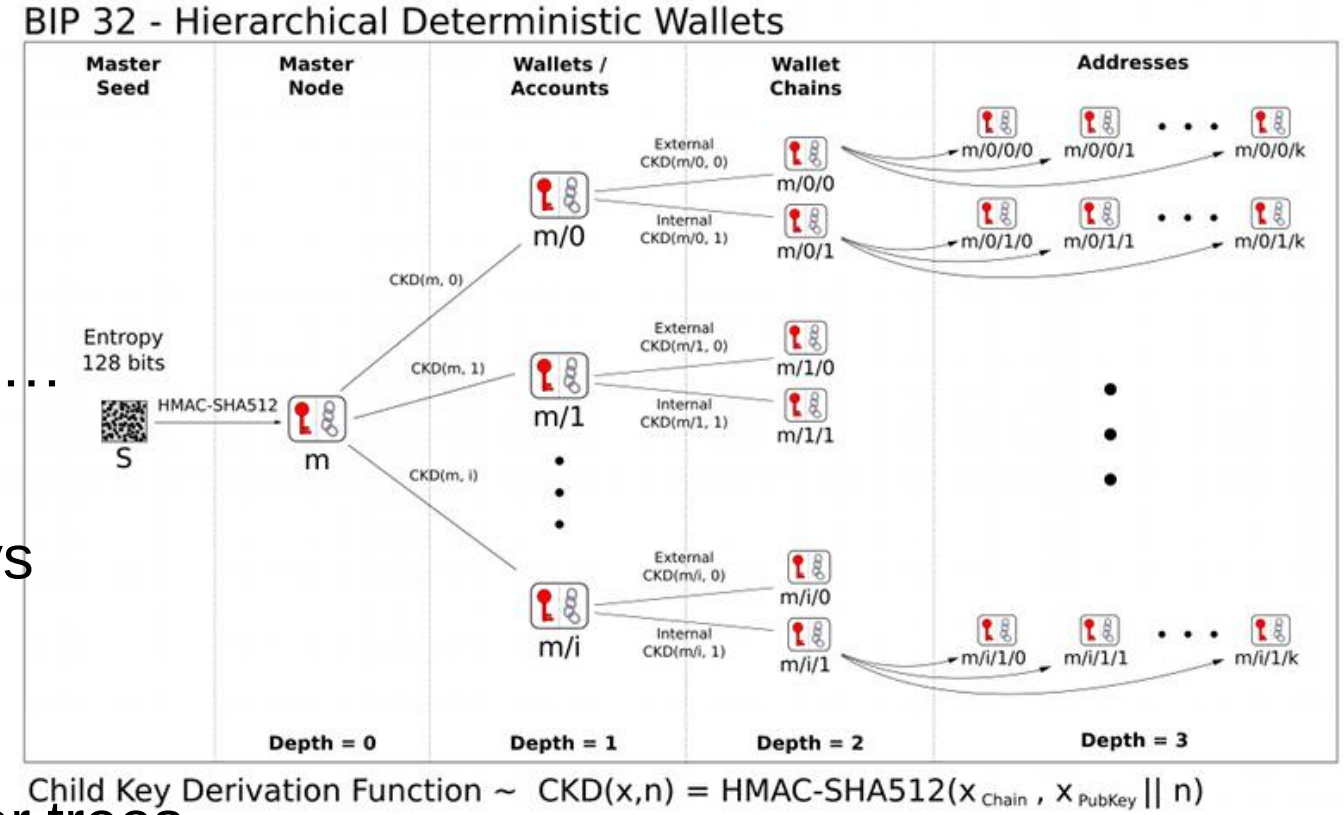
SINGLE-SIGNATURE WALLET

Backing up entropy (“master seed”)

- 128 or 256 bits of entropy
- How to store securely?
  - Write on paper, punch into metal plate, carve into stone…
  - How to prevent human typing error (bits → mnemonics, BIP39)
  - Do not write digitally (malware may steal)
- How to prevent single point of failure?
  - Make two copies (=> more robust against accidental loss)
  - Make (threshold) parts Shamir (=> more robust against intentional theft and loss - threshold)
  - Require multiple signatures (multisig, MPC)

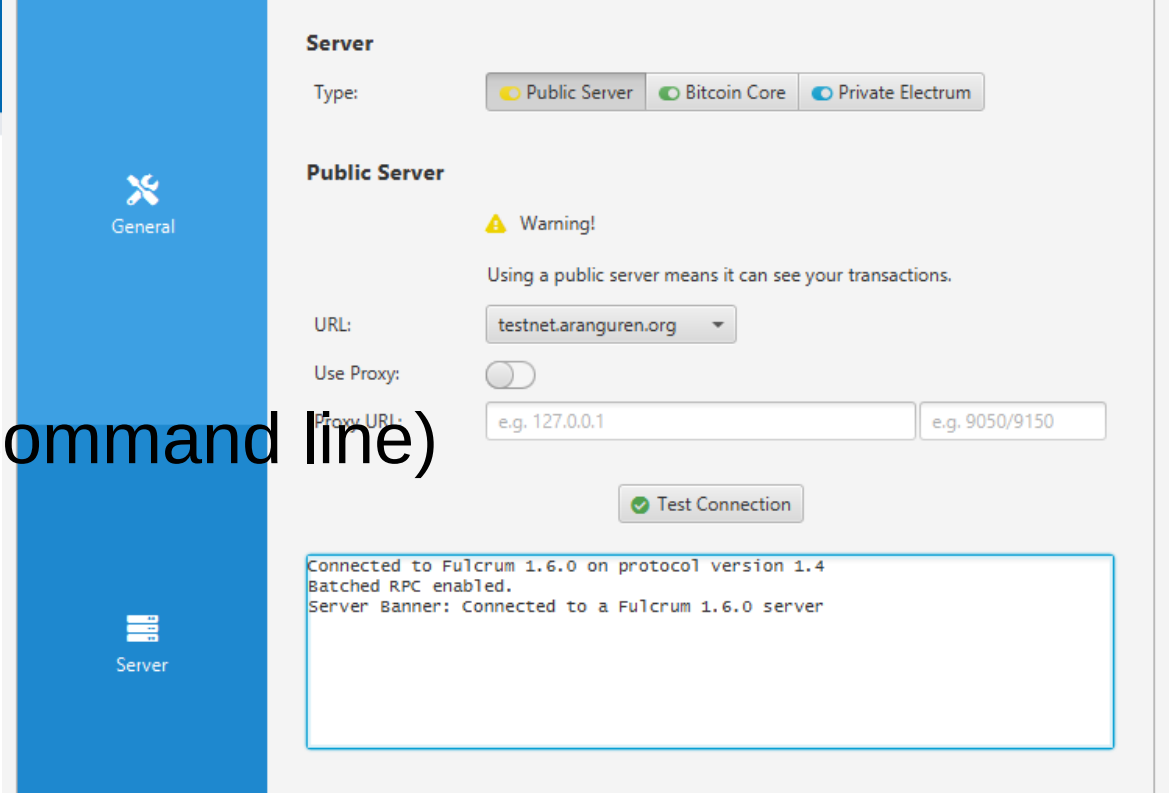
Making fresh private keys (with backup) BIP32, BIP44…

- Deterministic derivation from:
  - master seed (key)
  - derivation path (data)
    - m/purpose/coin/account/receive…
- Single master seed allows:
  - Generate many distinct private keys
  - Sharing sub-tree value allows:
    - Generate keys in sub-trees
    - Cannot generate keys from other trees
- Deterministic generation, Master Seed enough to recover whole tree



Starting Sparrow wallet

- Run your wallet with testnet switch (command line)
  - E.g., `./sparrow -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 ☺)

Generating new “wallet”

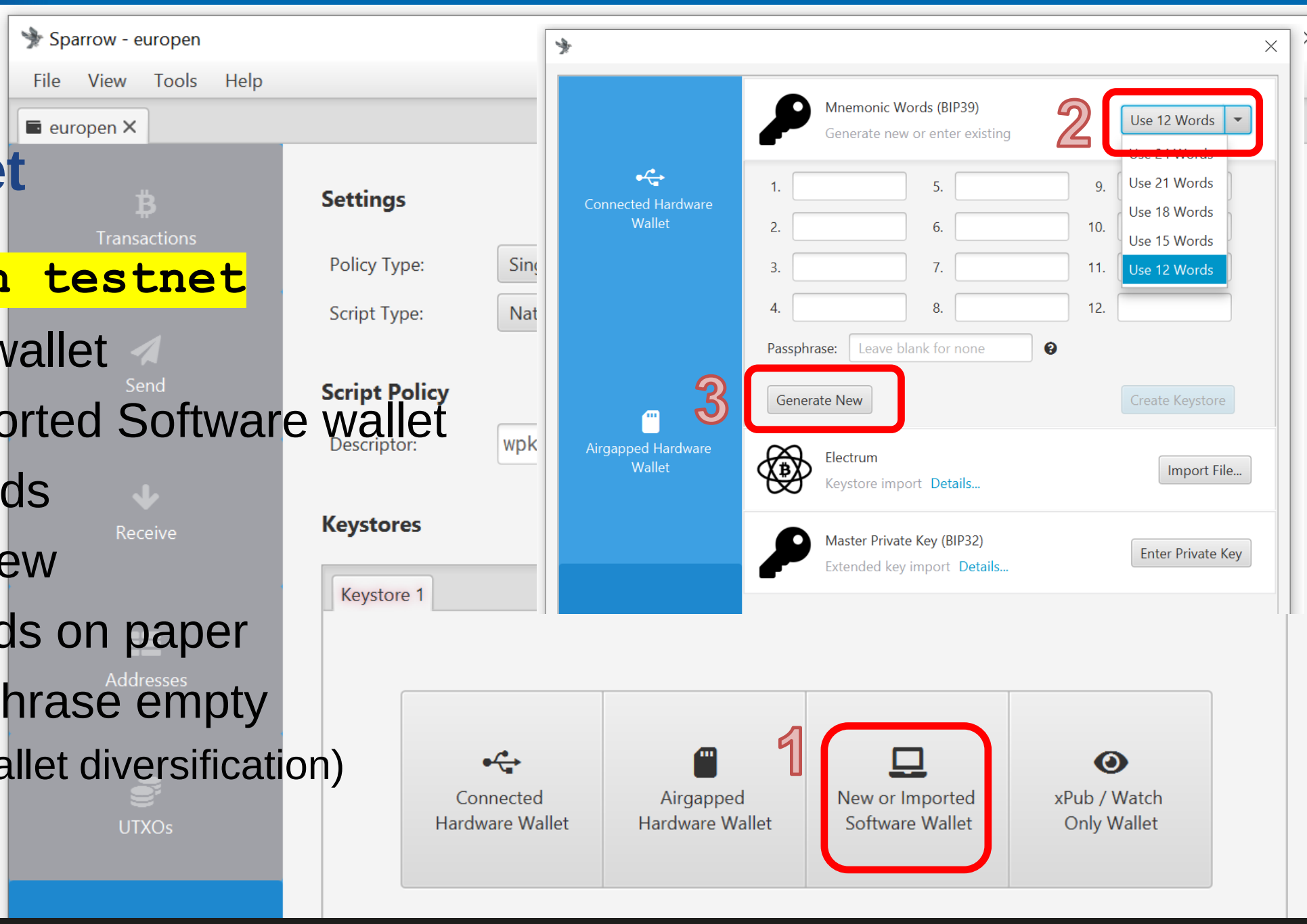
- A “wallet” is key management software controlling your private and public keys (ECDSA, Schnorr)
- The most important part of wallet is random number called root seed (128 or 256 bits)
- Root seed is used to deterministically generate practically unlimited number of keypairs
  - Specified in BIP32, “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

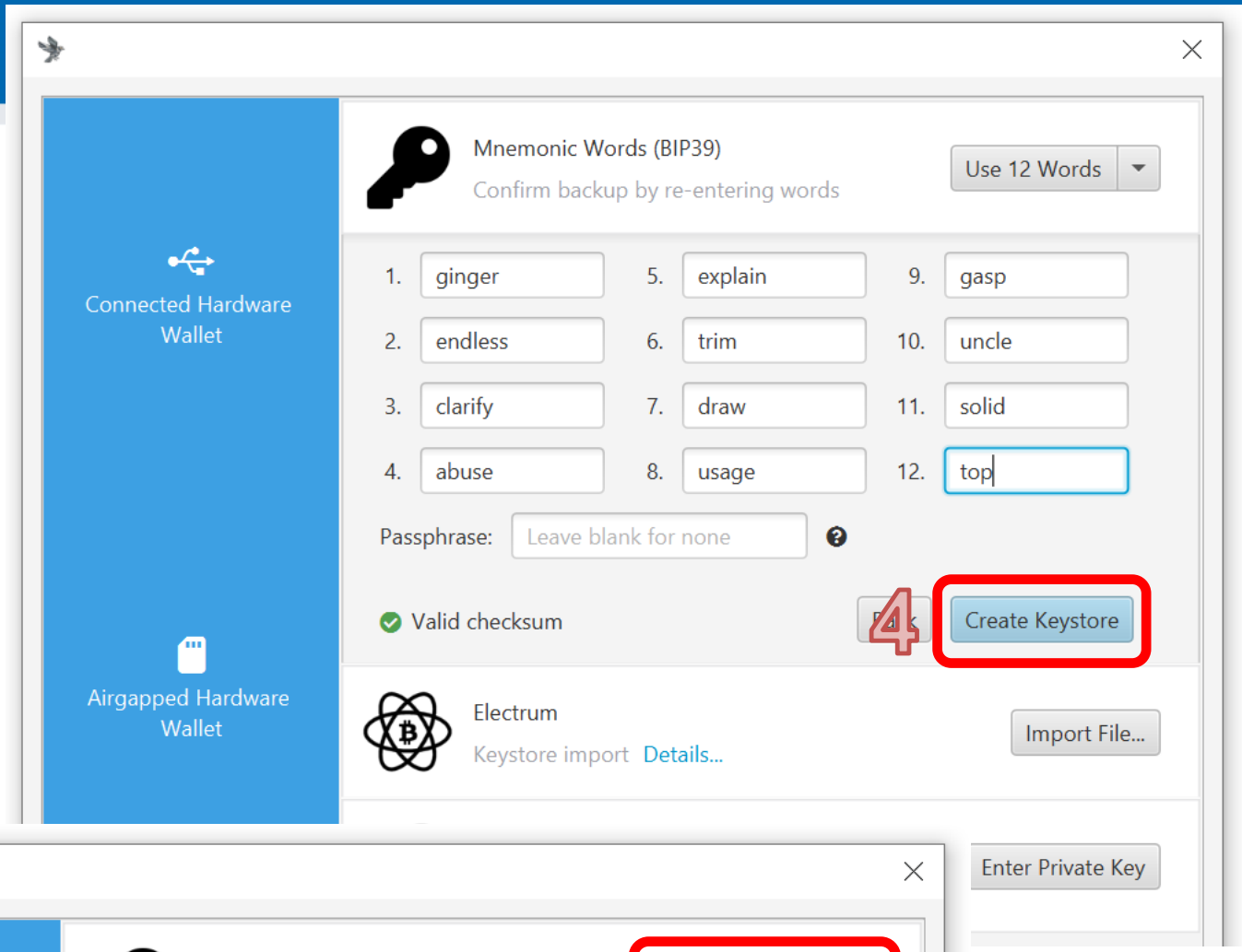
- Write 12 words on paper
- Leave Passphrase empty
  - (additional wallet diversification)

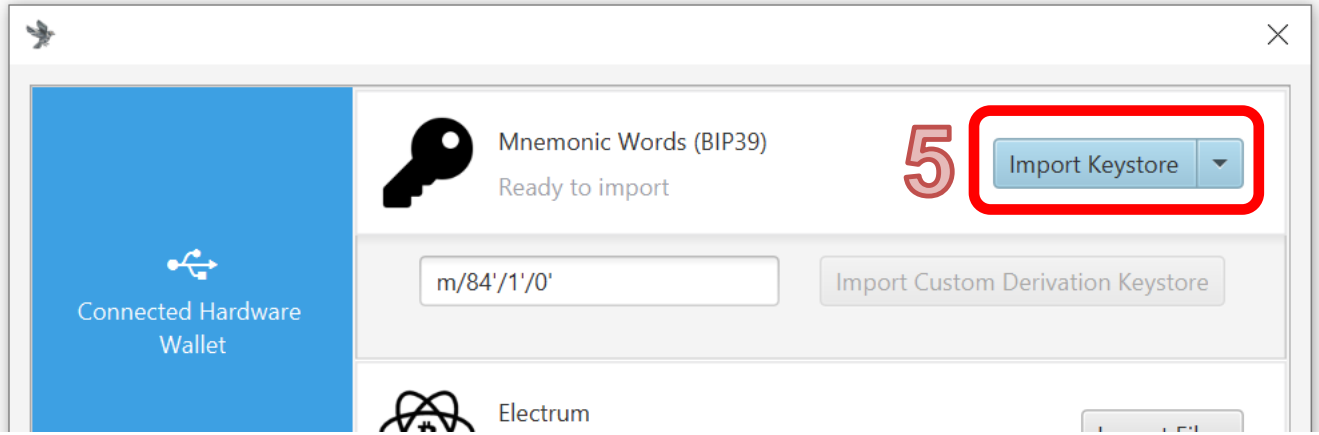


Create wallet

4. Create Keystore
- Confirm backup
- Reenter words

5. Import Keystore

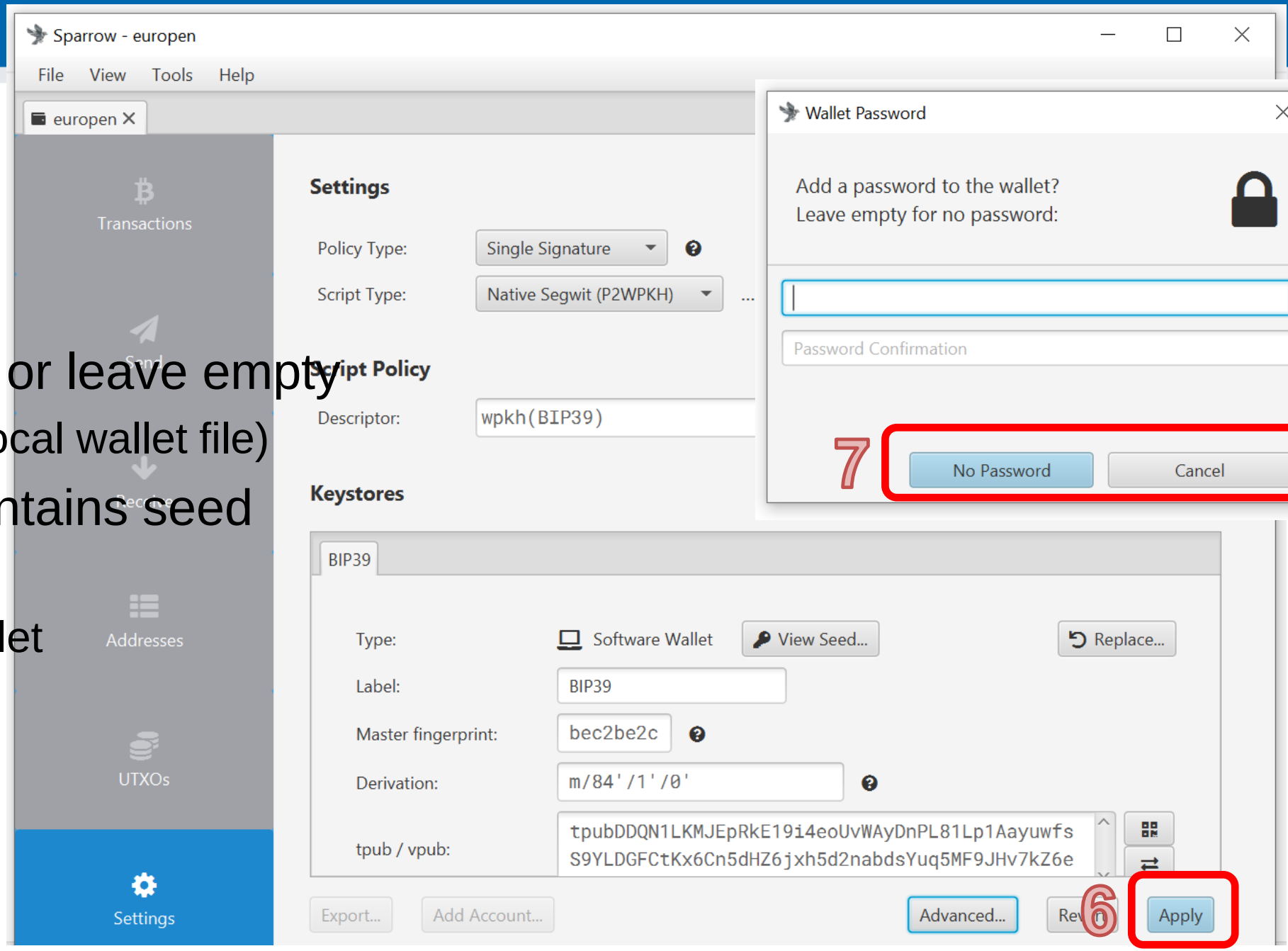




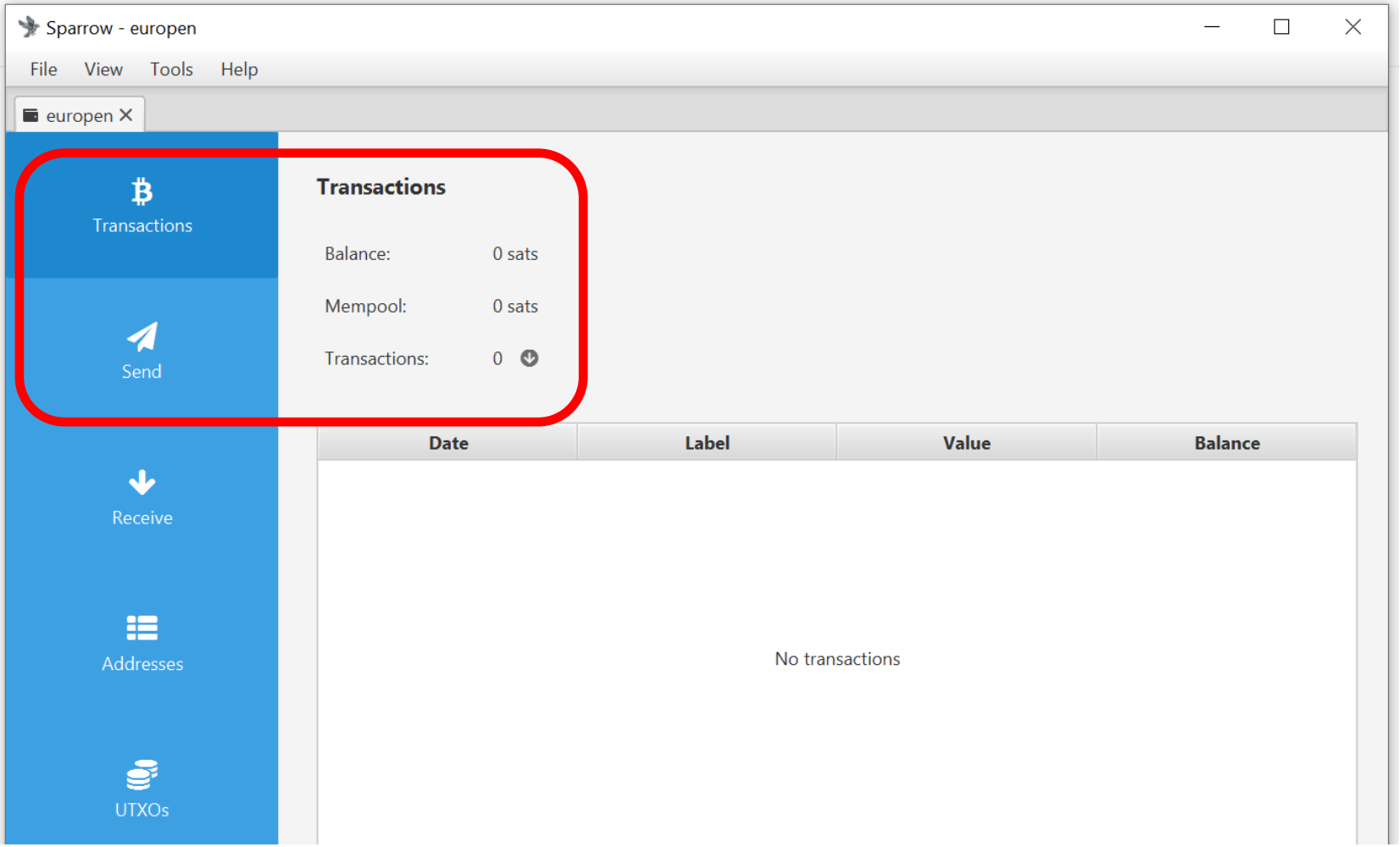
Create wallet

6. Apply
7. Set password or leave empty
   – (encryption of local wallet file)

- Local wallet contains seed
  – *.mv.db file
  – File→Open wallet



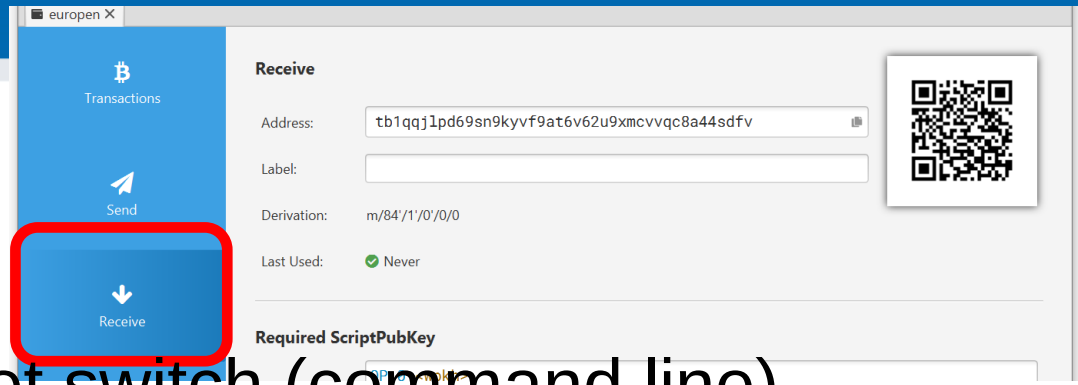
Wallet created (but empty ☺)



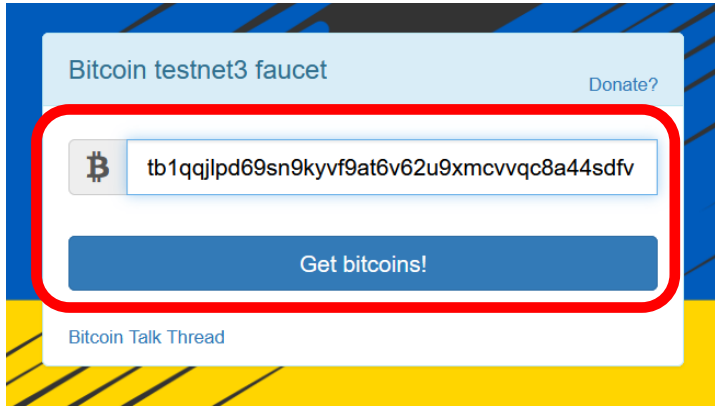
Receiving (testnet) bitcoins

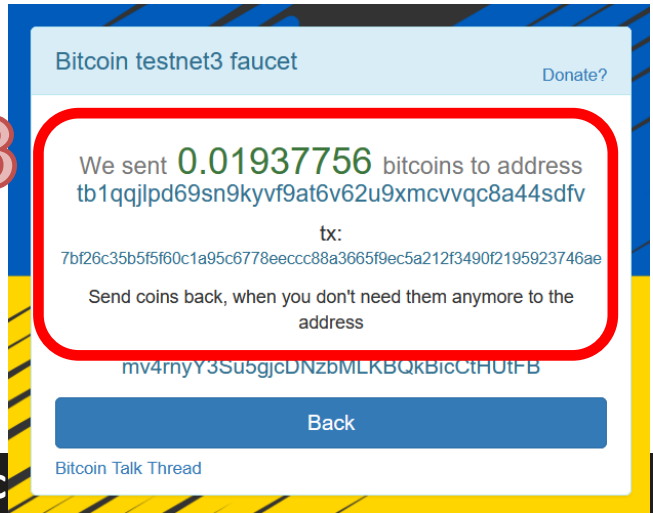
- You generate new “address”
  - deterministically derived from your root seed and fresh derivation path (path + counter) => new ECDSA keypair [BIP32]
  - public key X is pasted into locking script (“who can sign with private key verifiable with X can move bitcoin further”) and hashed => “address” [P2SH/P2WSH] (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)

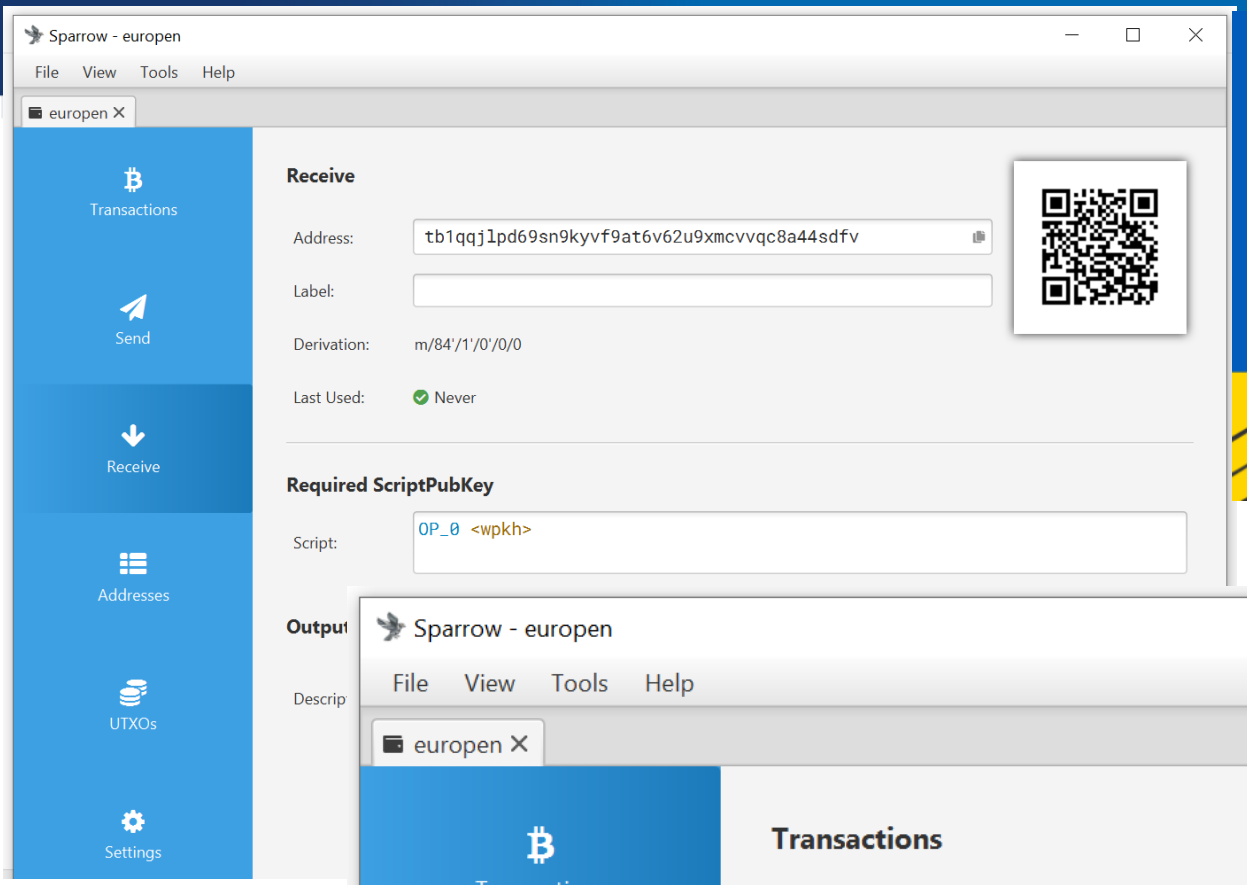
Getting test bitcoins (tBTC)

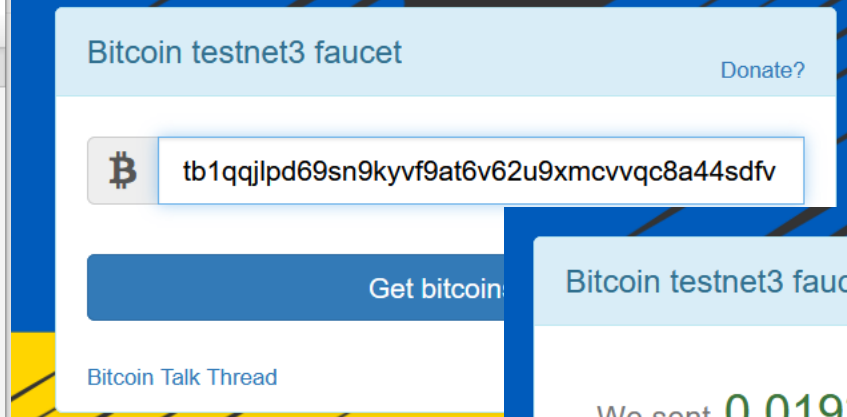


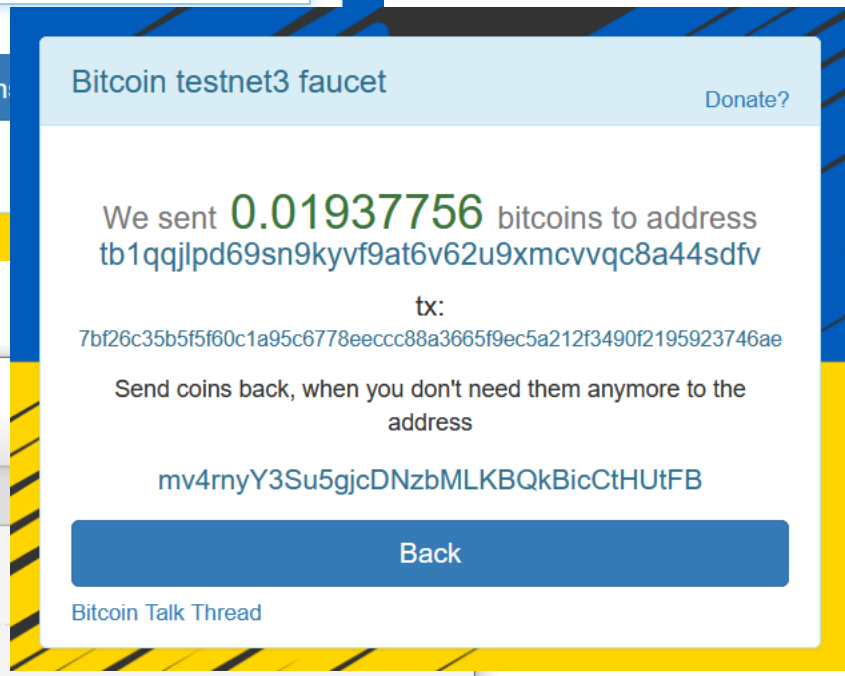
- If not running, run your wallet with testnet switch (command line)
  - E.g., **`./sparrow -n testnet`**
  - Generate new (testnet) receive address
- Go to https://coinfaucet.eu/en/btc-testnet/
  - Insert your testnet receive address
  - You may get more every 12 hours (per single IP)
  - (but please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

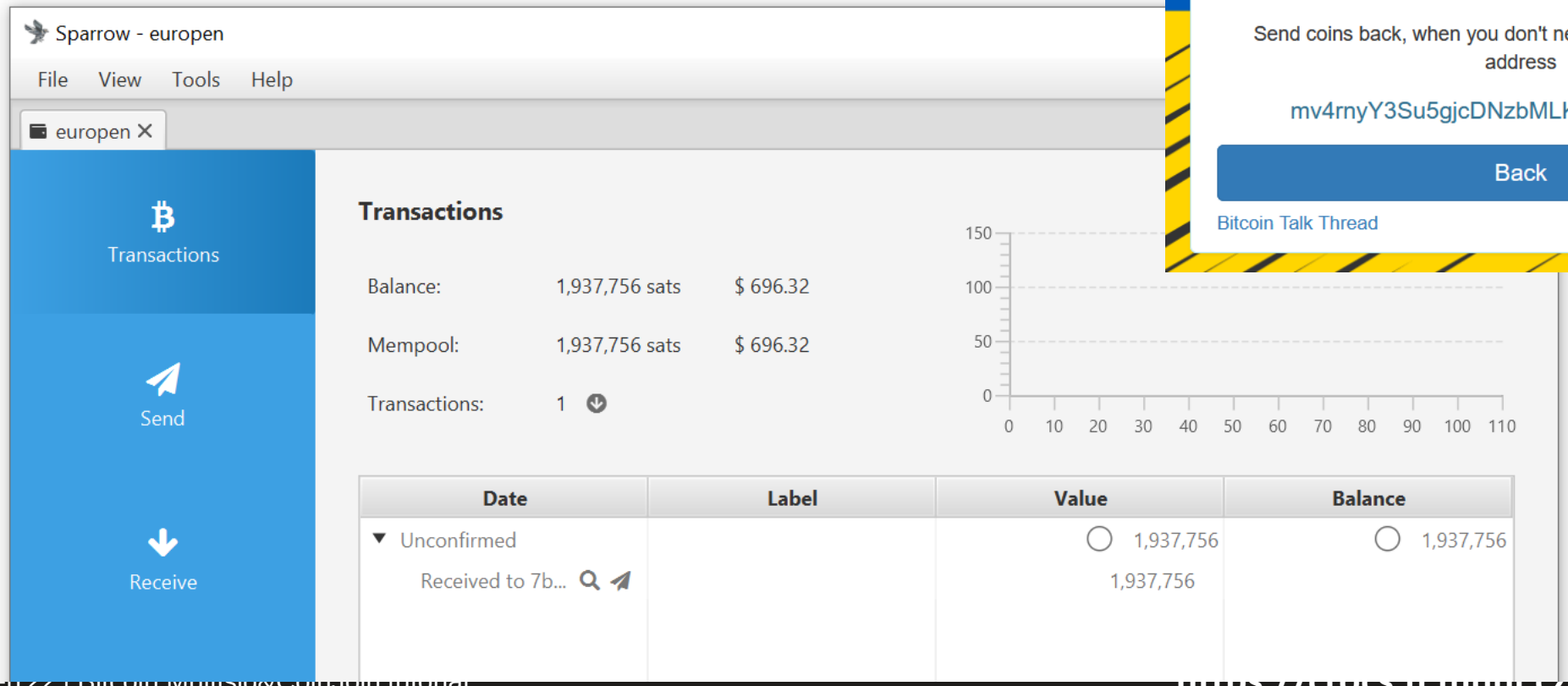





Sparrow - europen
File View Tools Help
europen
Transactions
Send
Receive
Addresses
UTXOs
Settings
Receive
Address: tb1qqjlpd69sn9kyvf9at6v62u9xmcvvqc8a44sdfv
Label:
Derivation: m/84'/1'/0'/0/0
Last Used: Never
Required ScriptPubKey
Script: OP_0 <wpkh>
Output
Descrip


Bitcoin testnet3 faucet
Donate?
tb1qqjlpd69sn9kyvf9at6v62u9xmcvvqc8a44sdfv
Get bitcoin
Bitcoin Talk Thread


Bitcoin testnet3 faucet
Donate?
We sent 0.01937756 bitcoins to address
tb1qqjlpd69sn9kyvf9at6v62u9xmcvvqc8a44sdfv
tx:
7bf26c35b5f5f60c1a95c6778eeccc88a3665f9ec5a212f3490f2195923746ae
Send coins back, when you don't need them anymore to the address
mv4rnyY3Su5gjcDNzbMLKBQkBicCtHUtFB
Back
Bitcoin Talk Thread


Sparrow - europen
File View Tools Help
europen
Transactions
Send
Receive
Transactions
Balance: 1,937,756 sats $ 696.32
Mempool: 1,937,756 sats $ 696.32
Transactions: 1
150
100
50
0
0 10 20 30 40 50 60 70 80 90 100 110
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

Explore your transaction

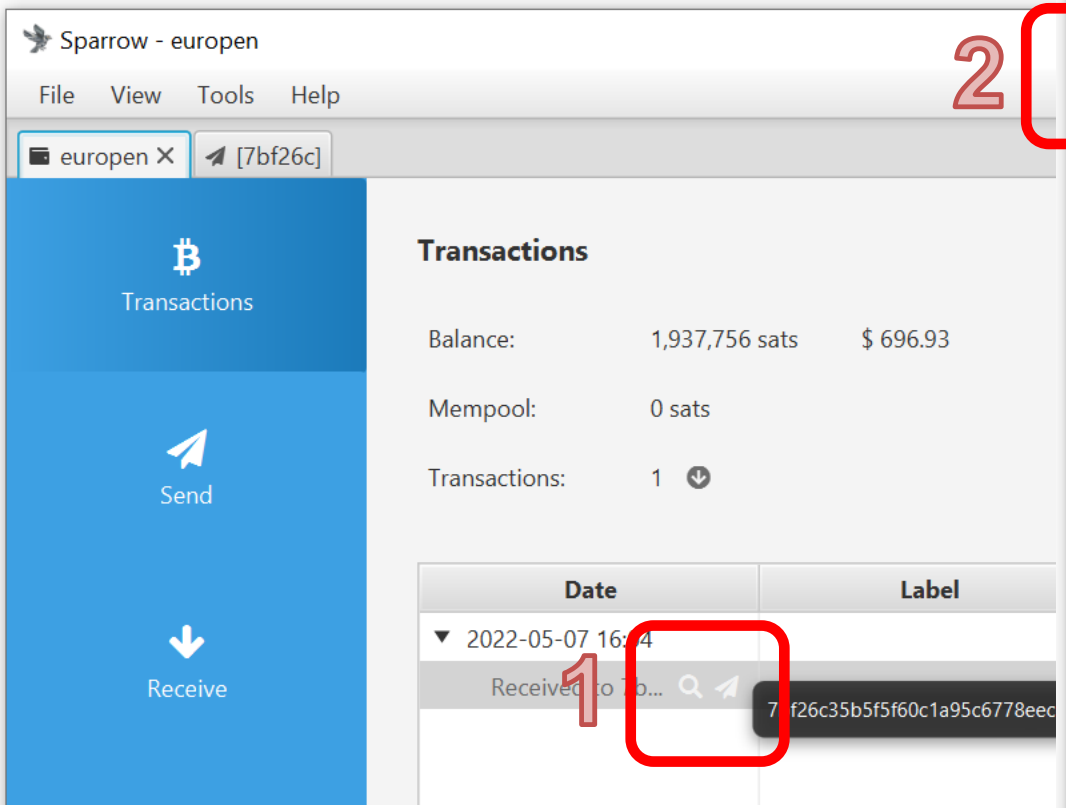
I. Analysis using Sparrow wallet

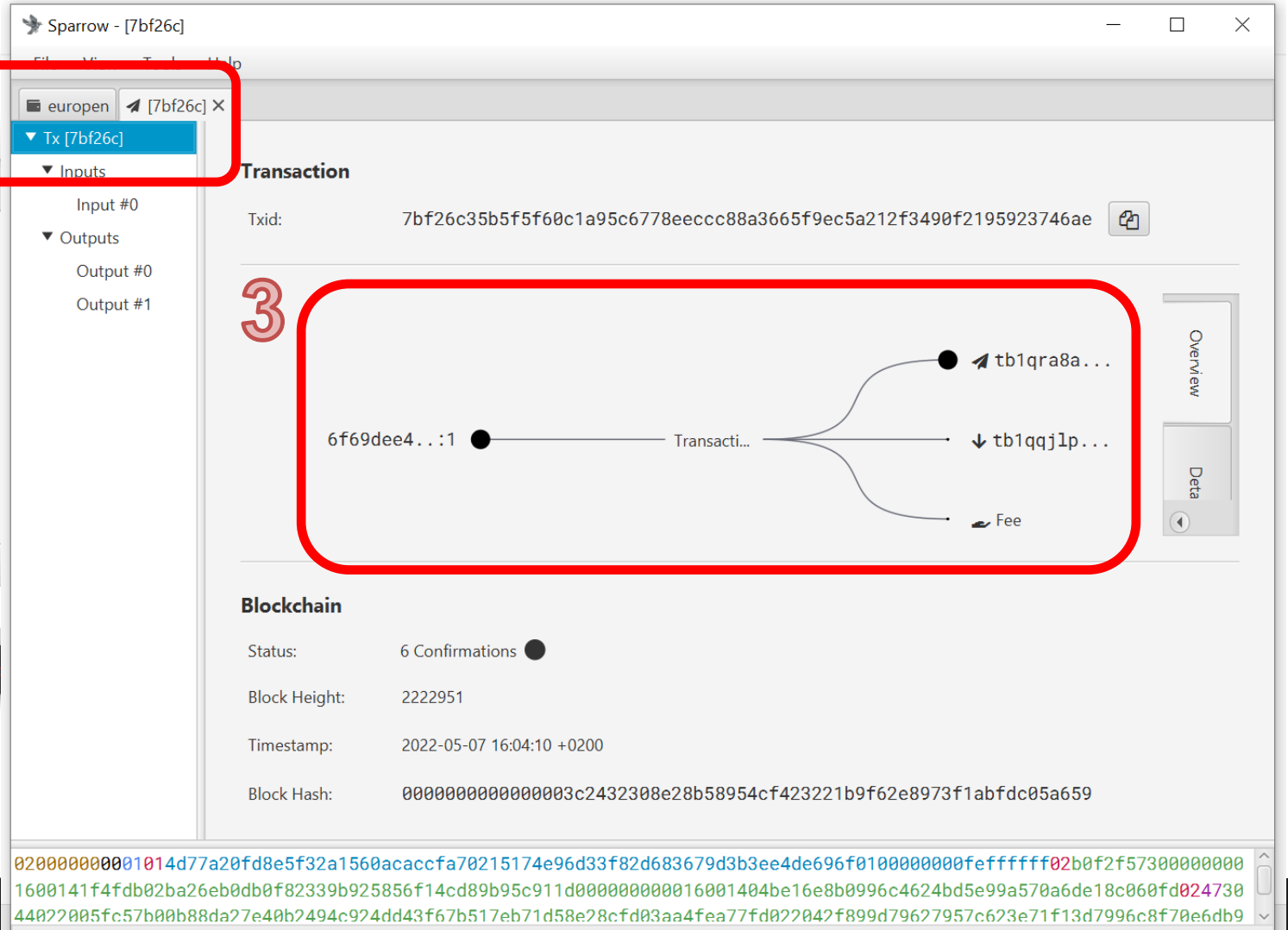
1. Click Transactions tab, magnifier symbol
2. Select topmost element on left TX [xxxxxx]
3. Visualization of transaction including fee (more details)

II. Analysis using public blockchain explorer

– Visit https://blockstream.info/testnet/
– Paste your address or tx ID from coinfaucet
– More details by DETAILS + button

Transaction analysis using Sparrow wallet





Example of transaction analysis using block explorer

- More details DETAILS +
- Unlockscript (WITNESS)
- Lockscript (SCRIPTPUBKEY)

- Example:
  - In: 19.47472649 tBTC
  - Change: 19.45498288 tBTC
  - To us: 0.01937756 tBTC

https://blockstream.info/testnet/tx/7bf26c35b5f5f60c1a95c6778eeccc88a3665f9ec5a212f3490f2195923746ae

UTXO, coin control and privacy

- Your wallet needs to connect to service monitoring blockchain to establish not yet spent transactions (UTXOs) you control (e.g., Electrum Server software)
  - Your “balance” is sum of values of all UTXOs for which your wallet controls private keys (allowing to create valid unlock script)
- When paying some amount, some of your UTXOs need to be used as inputs to new transaction (becoming then spend TXs)
  - Wallet software may automatically select UTXOs which will be used (various strategies like best fit, lowest fee, oldest first, random…)
  - You can also select specific UTXO manually (aka coin control), labeling your UTXO helps to remember the source
- If you will use particular UTXOs to pay someone, it is then paired with your identity, revealing how much your own on that specific address
  - Creating fresh keypairs => address improves your financial privacy
  - If you use two UTXOs to pay and someone already attributed one address to you then he may assume that the second input is also yours (only heuristics, but very frequent)
  - CoinJoin and PayJoin are methods how to break this heuristics
- Label your UTXOs and use coin control to limit leakage about your total finds

Display funds (UTXOs) controlled by your wallet

- Your wallet controls private keys and corresponding public ones

1. Click UTXO tab
2. Observe Balance (in sats)
   - Total sum for UTXO you control (both confirmed and not yet confirmed)
   - Observe Mempool (in sats) – sum of UTXO not yet mined (unconfirmed)
3. Observe list of UTXOs below
   - Can click for more details
   - Can spend only selected UTXO (good for privacy)

Transactions

Balance:	2,442,190 sats	$ 878.39
Mempool:	504,434 sats	$ 181.43
Transactions:	2	

Date
2022-05-07 16:04
Received to 7bf...
Unconfirmed
Received to 65...

Transactions

Send

Receive

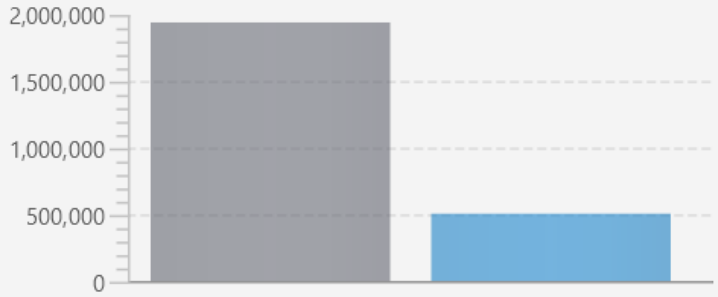
Addresses

1 UTXOs

Unspent Transaction Outputs

2

Balance:	2,442,190 sats	$ 878.39
Mempool:	504,434 sats	$ 181.43
UTXOs:	2	



3

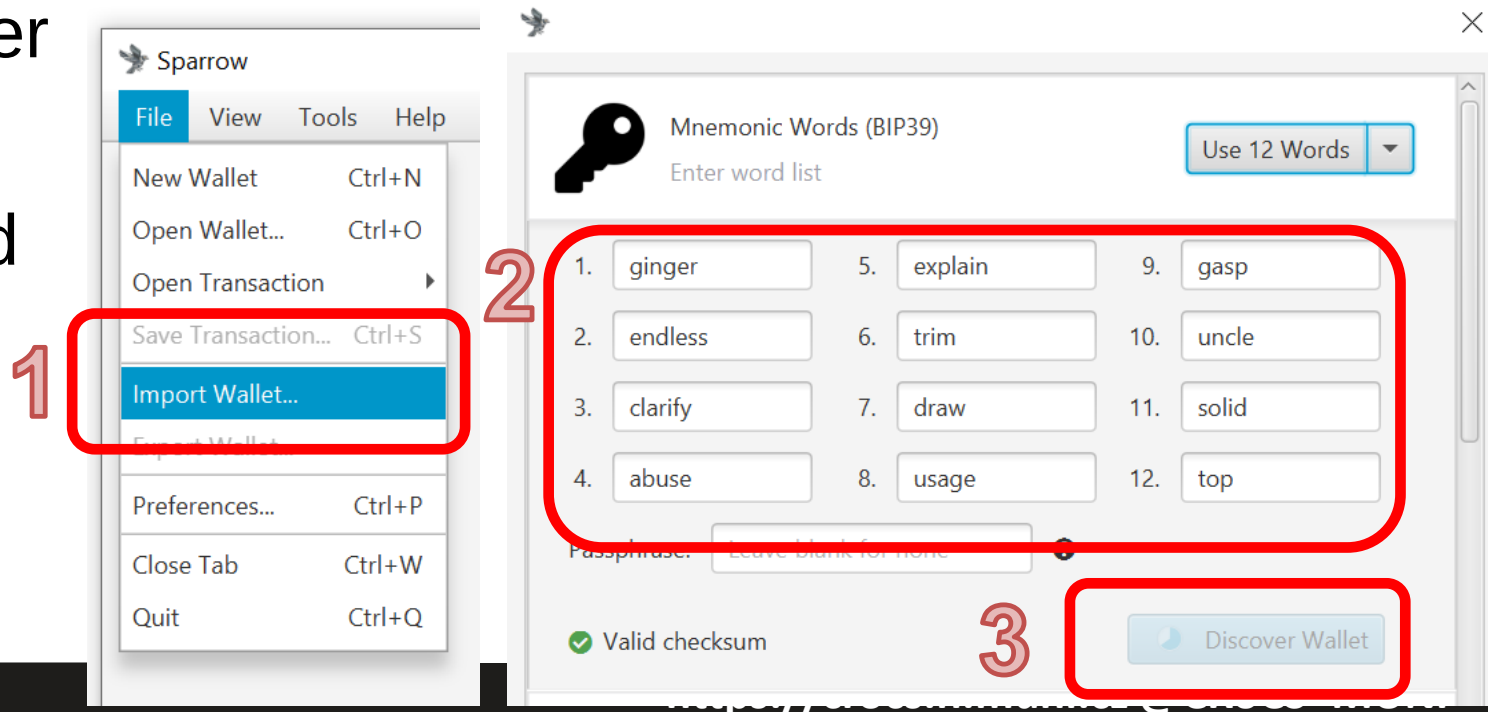
Date	Output	Address	Label	Value
2022-05-07 16:04	7bf26c35..:1	tb1qqjlpd69sn9kyvf9at6v62u9xmcvvqc8a4...		1,937,756
Unconfirmed (Spenda...	65edf1eb..:1	tb1qj5m9kwp3ja37kg2lns0jrsxgu4rgqd6kv...		504,434

Wallet recovery

- Make sure your 12/24 mnemonic words are written on paper
- Close previously created wallet (or even delete wallet file *.mv.db)

1. File → Import wallet → Mnemonic Words (BIP39)
2. Type words in correct order
3. Discover wallet

- Wallet txs are synchronized
  - (from connected fullnode)



Wallet recovery

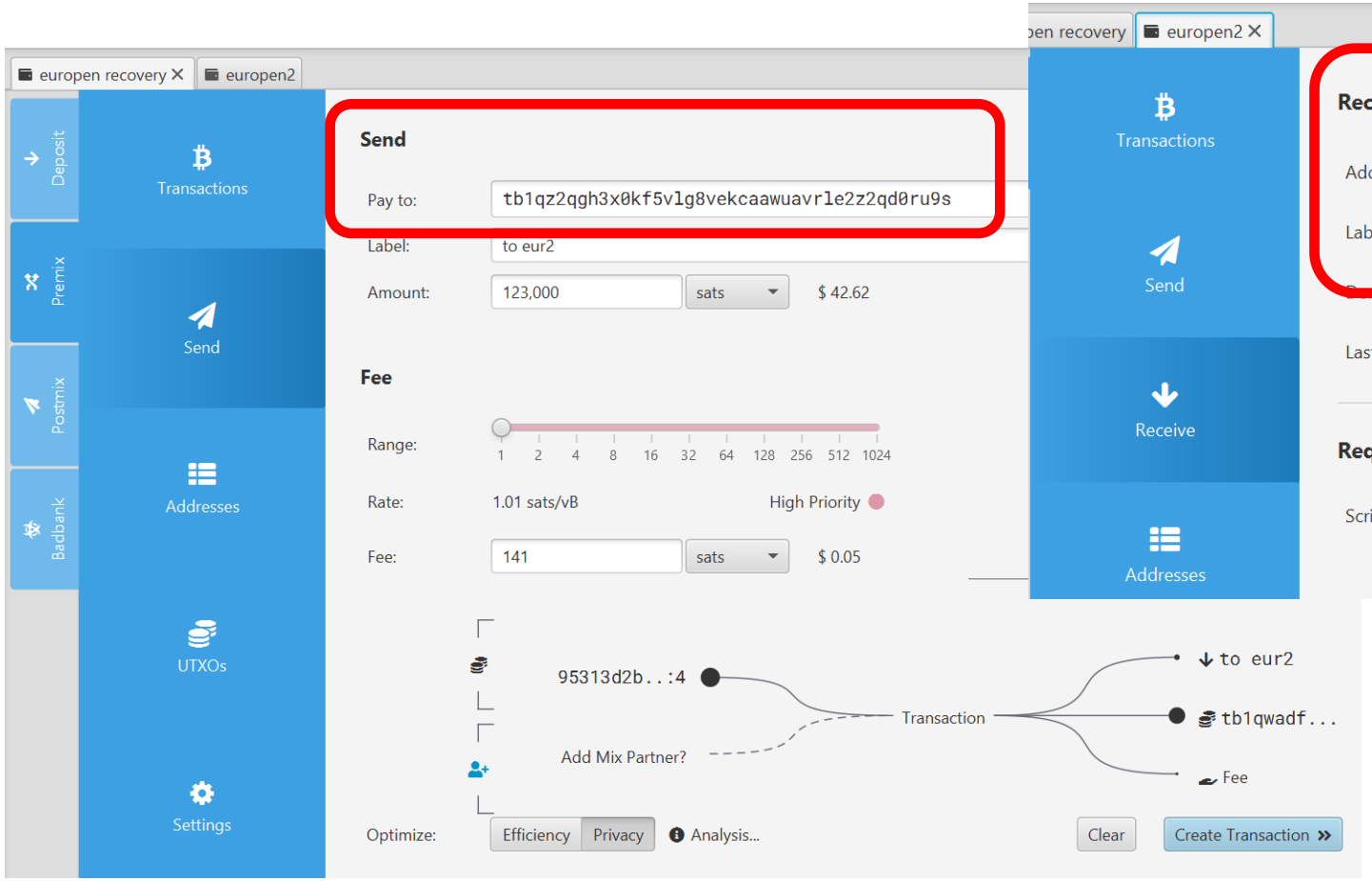
- The control of all funds (== private keys to UTXOs) can be recovered from root seed and some additional (somewhat public) information
  - Root seed contains all the entropy (most important)
  - Also derivation path and used type of lock scripts (somewhat public)
  - Not all wallets use same derivation path, see most common here https://walletsrecovery.org/
- Recovery equals to:
  - Creating new wallet but with previous root seed instead of new random one
  - Searching for addresses generated from this root seed (for derivation path + counter)
    - Counter is incremented as long as transactions are found on blockchain
  - Search stops when number of unused future addresses (“gap limit”) are tested and not found
- Additional metadata like UTXO labels are lost
- When backing root seed, write down also wallet version (or script policy descriptor)

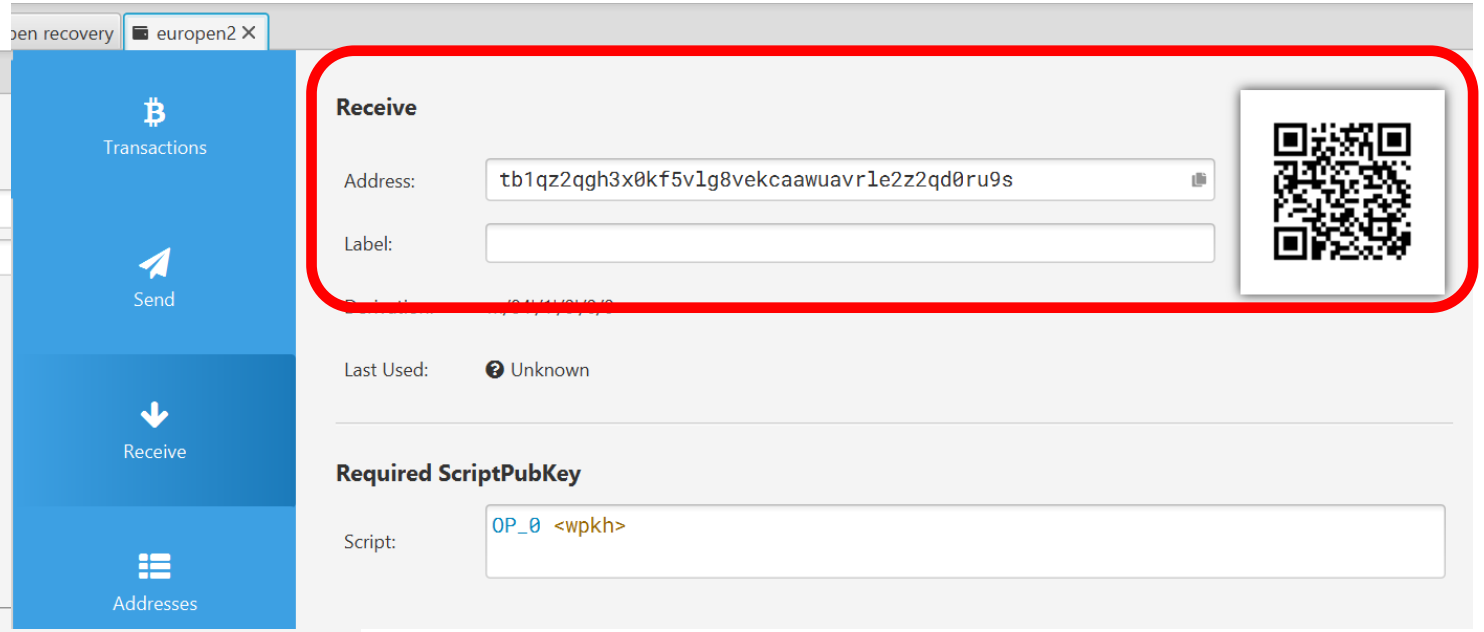
Task: send some tBTC to your peer

- 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

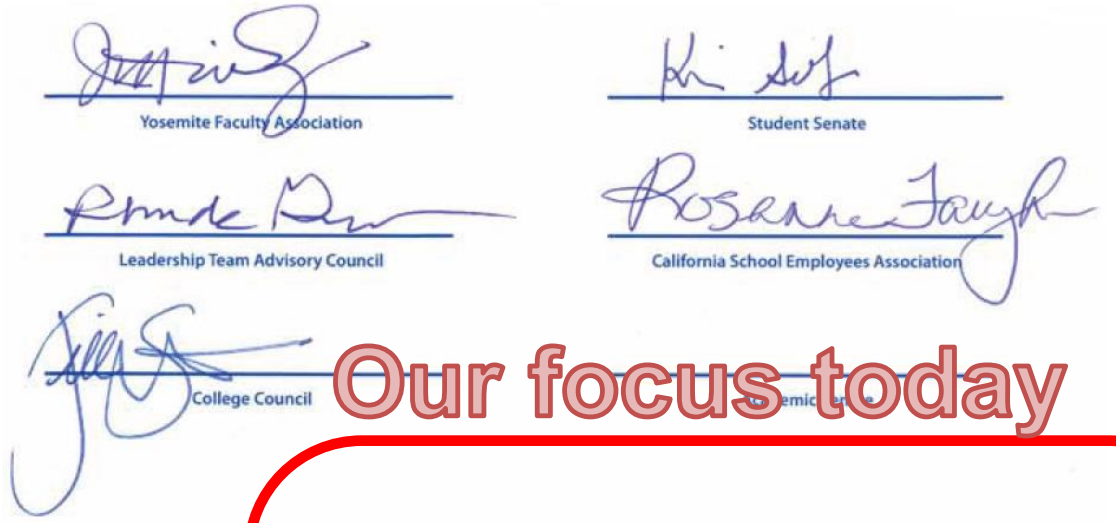

europen recovery
europen2
Deposit
Premix
Postmix
Badbank
Transactions
Send
Addresses
UTXOs
Settings
Send
Pay to:
tb1qz2qgh3x0kf5vlg8vekcaawuavrle2z2qd0ru9s
Label:
to eur2
Amount:
123,000
sats
$ 42.62
Fee
Range:
1 2 4 8 16 32 64 128 256 512 1024
Rate:
1.01 sats/vB
High Priority
Fee:
141
sats
$ 0.05
95313d2b..:4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


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

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?

MULTISIG

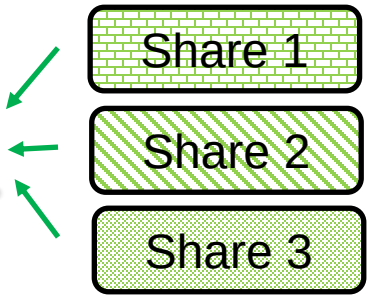


Analogically for decryption (single person decrypts, multiple people, k-of-n)

Our focus today

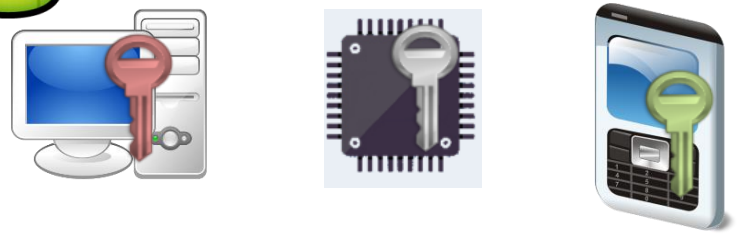
Single signature

Shamir TSS



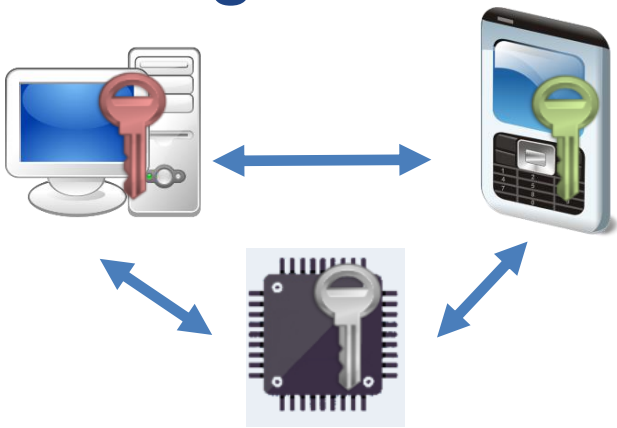
Signature

Multiple signatures



Signature | Signature | Signature

MPC signature



Signature

1. THRESHOLD SECRET SHARING
2. MULTISIGNATURES
3. MULTI-PARTY CRYPTO COMPUTATION

1. Shamir's threshold secret sharing scheme

- Private key is recovered from multiple shares
  - Then used at single place
  - An attacker can compromise private key after its recovery from shares
- Network is unaware of key split, single public key used in lock script
- Can be used to backup wallet seed (e.g., Trezor wallet https://trezor.io/shamir/)
  - n-out-of-n or k-out-of-n

Single Backup vs. Shamir Backup

https://trezor.io/shamir/

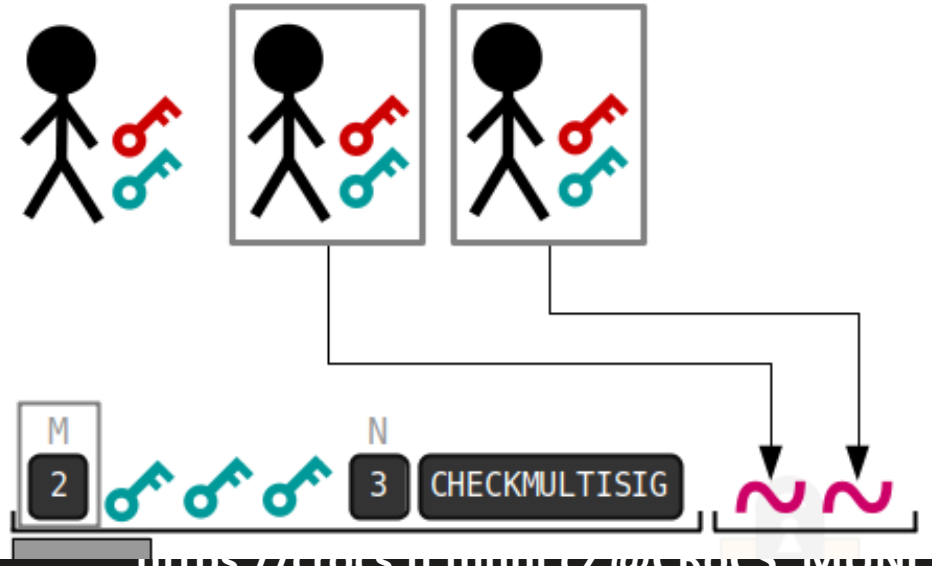
Single Backup Safe

Shamir Backup Even safer!

Master Seed	A single recovery seed	Up to 16 recovery shares
Seed Words	12, 18 or 24 word recovery seed	20 or 33 words in each share
Advantages	Easy to manage	Choose your threshold
Recovery	Independent control of recovery seed	Administrative control of master seed
Independence	Autonomous control of assets	Autonomous control of assets
Security	Secure offline backup of private keys	Secure offline backup of private keys
Extra Security		Eliminated risk of theft or loss

2. Multisignatures

- Lock script constructed to require multiple signatures (OP_CHECKMULTISIG)
  – transaction valid only if multiple signers provide signatures for unlock script
- n-out-of-n or m-out-of-n, https://en.bitcoin.it/wiki/Multisignature
- P2MS, P2MS wrapped in P2SH
  – https://learnmeabitcoin.com/technical/p2ms

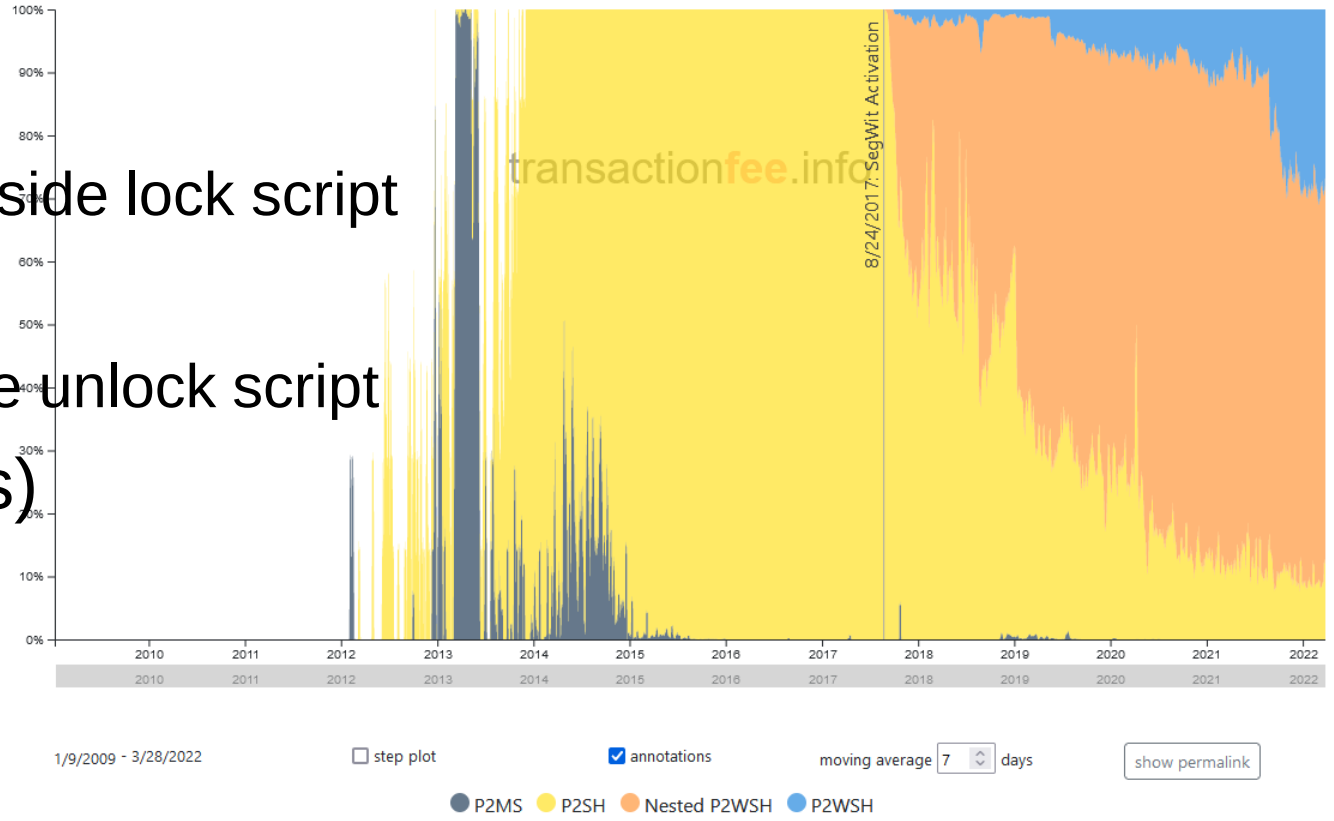


3. Secure multi-party computation (MPC)

- Single signature computed using multiple separated signers
  - Each signer has own private key
  - An attacker must comprise more than one entity
- Communication between signers
  - During initial key generation
  - Optionally during signing
- Legacy compatible schemes (produces valid ECDSA signature)
  - 2-party ECDSA, n-out-of-n or k-out-of-n ECDSA (only since 2016)
- Taproot-compatible schemes (activated since Nov 2021)
  - Schorr signatures, MuSig2, Myst, SHINE, FROST…
- https://academy.binance.com/en/articles/threshold-signatures-explained

Frequency of different multisignature scripts

- Cannot tell for Shamir, MPC ECDSA and Schnorr (e.g., MuSig)!
  - Resulting signature is standard signature, no change to lock/unlock scripts
    - Good for privacy!
- Can tell for P2MS
  - Threshold + allowed public keys inside lock script
- Can tell for P2SH (if spent)
  - Multisig script and used keys inside unlock script
- (analogically for Segwit variants)



Multisignature

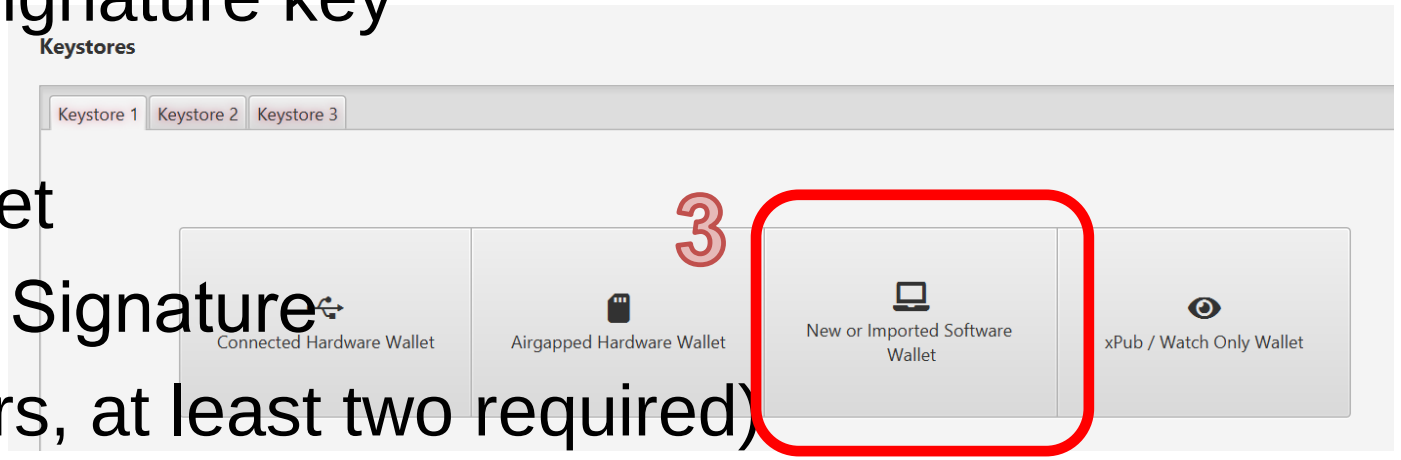
- Different signers can use different wallet software and/or hardware wallets
  - Results in better security in case of software vulnerability in specific wallet
- Different signers can be in different geographical locations
  - Theft/physical coercion at one place will not be enough
- Sparrow wallet is acting as signing coordinator
  - Typically, one private key on particular machine and xpubs from other signers
    - Can generate new addresses, can coordinate spend (signing via PSBT)
- New “address“ is created as script locking to all group members
  - All members also see the current balance of the multisig wallet (implication for privacy)

Task: Create multisignature wallet

- Form groups of three members
  - (can be also done with three Sparrow instances on same machine – for testing)
  - Make sure you can send short messages to each other (Signal) or have camera read QR codes
- Quorum 2-out-of-3 will be used (3 members, 2 enough to authorize)
- Every participant will create one keystore with knowledge of private key(s) and then import remaining two xpubs (tpubs on testnet) for other two signers
- Some tBTC will be send to multisig wallet
- Cooperation of two members will be used to create new transaction

Create multisignature wallet I.

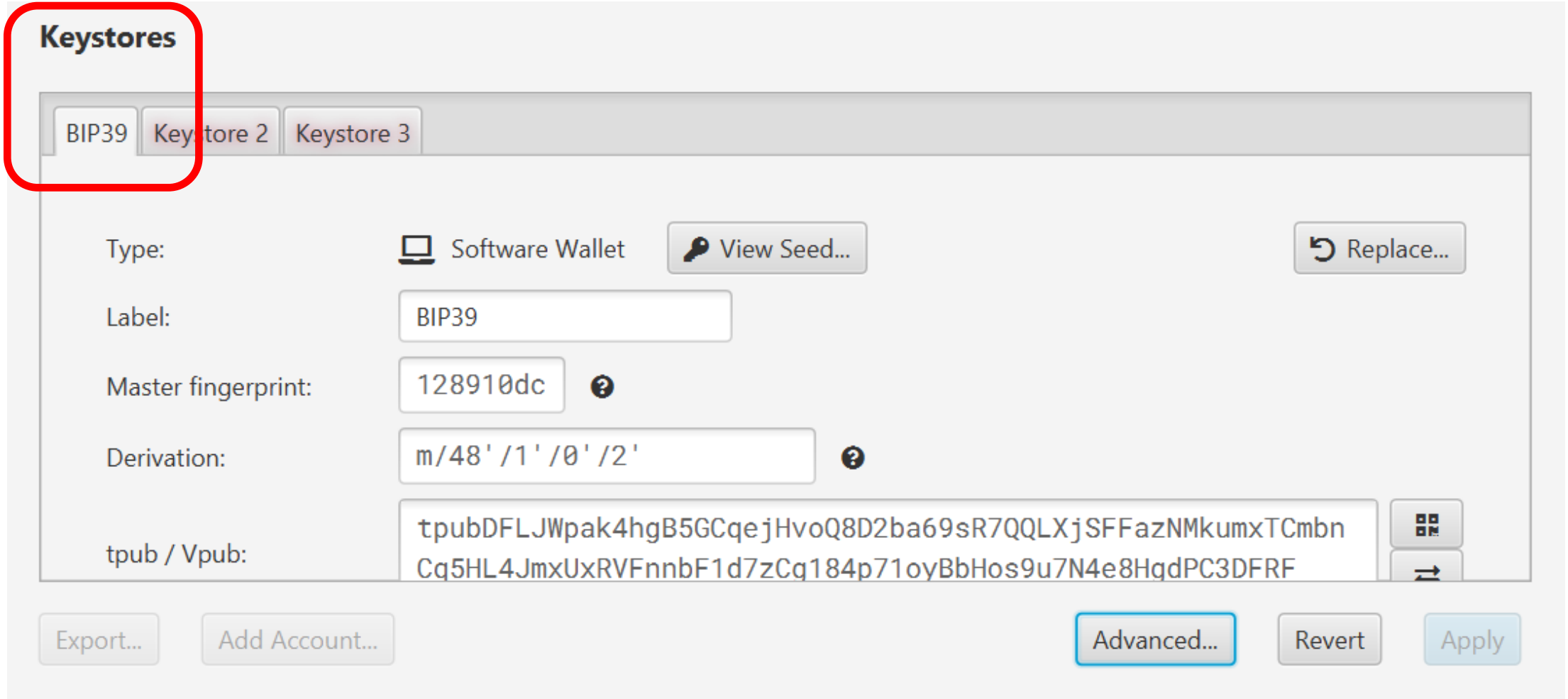
- Every participant creates one signature key
- File → New wallet
- New or Imported Software wallet



1. Change ‘Policy Type:’ to Multi Signature
2. Set M of N to 2/3 (three signers, at least two required)
3. Set Keystore 1 as ‘New or Imported Software wallet’
4. Setup Keystore 1 as before (singlesig wallet, 12 words, Import keystore)

Keystore 1 now created

4



Create multisignature wallet II.

- Insert xpubs/pubs for other two signers (your group members)

5. Transfer tpub from your Keystore 1 to other two members (Signal/QR code)
   - Paste received tpubs into Keystore 2 and 3 (select ‘xPub / Watch Only Wallet’)
6. Set Derivation same as for Keystore 1 (m/48'/1'/0'/2’)
   - For both Keystore 2 and Keystore 3
7. When all three keystores are filled, Apply button is enabled (click it)
8. Let one member to send some tBTC to multisig wallet
   - Receive, send from singlesig wallet (do not send all funds)
   - All members shall see new tBTC coming to multisig wallet

Keystores

BIP39 | Keystore 2 | Keystore 3

Type: Software Wallet — View Seed...

Label: BIP39

Master fingerprint: 128910dc

Derivation: m/48'/1'/0'/2'

tpub / Vpub: tpubDFLJWpak4hgB5GCqejHvoQ8D2b
Cq5HL4JmxUxRVFnnbF1d7zCg184p71

Export... Add Account...

Keystores

BIP39 | Keystore 2 | Keystore 3

Type: Watch Only Wallet — Import...

Label: Keystore 2

Master fingerprint: 00000000

Derivation: m/48'/1'/0'/2'

5

tpub / Vpub: tpubDFLJWpak4hgB5GCqejHvoQ8D2ba69sR7QQLXjSFFazNMkumxTCmbnCq5
HL4JmxUxRVFnnbF1d7zCg184p71oyBbHos9u7N4e8HgdPC3DFRF

Keystores

BIP39 | Keystore 2 | Keystore 3

Type: Watch Only Wallet — Import...

Label: Keystore 3

Master fingerprint: 00000000

6

Derivation: m/48'/1'/0'/2'

tpub / Vpub: tpubDEbH1xDZn981WBe736Bc2Ps2Hp8941f69ckMptWL9F
1cJEqir7Hpknxnzr63iGd1Zq1Tm8K1Km7Fv3xDeEeZPduJ

rivation: m/48'/1'/0'/2'

ub / Vpub: tpubDED2dnYnViJHDyoTpexKab5iVxKS9uH2iE5HHZvfdFVPbHvzDxHXL2c2
iQJCwN6R4sqBrbhmKvdnDPMQk8mEvRGwMSvMqPNiVnNmMPc3u5w

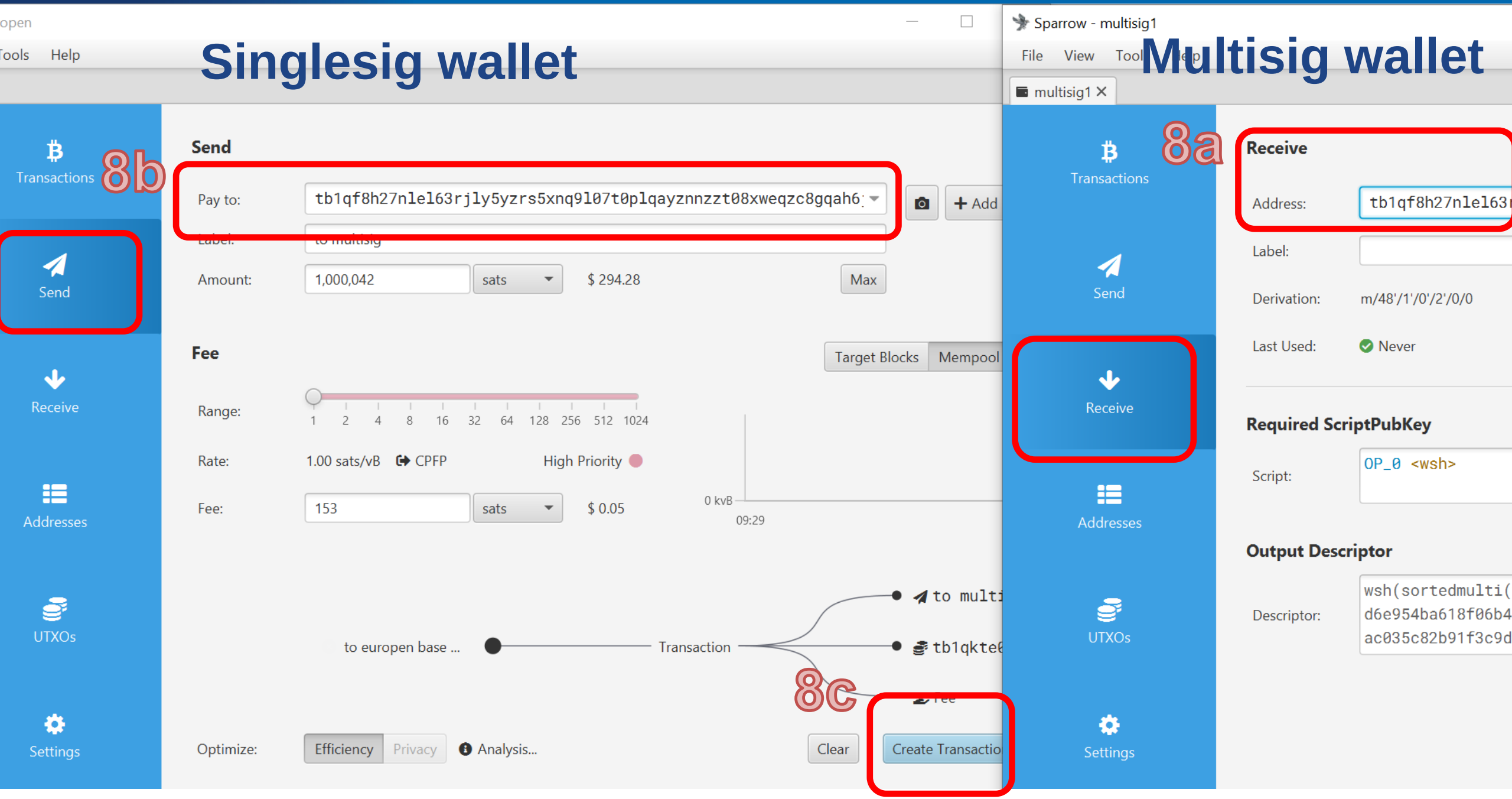
Add Account... Advanced... 7 Revert Apply

Broadcasting the transaction

- New transaction is created locally on your computer, can be offline
  - Even chain of transactions spending from the previous ones
  - Local transactions can be serialized to binary blob and transferred to other computer/users (file, QRCode, NFC…)
  - Transaction is not mined, so other users are unaware of it (and can't verify)
- By broadcasting the transaction publicly, the network is notified, and transaction can be mined into some future block
  - Broadcast is done via Bitcoin P2P messaging network, between fullnodes
  - New transaction is added to local Mempool of a fullnode and broadcasted further
    - No global Mempool exists (only many local ones), but synchronized usually within seconds
- Broadcast can be done via fullnode you are connected to or via third-party node
  - Protect IP of your fullnode (first node to broadcast – likely originator/owner of transaction)
  - E.g., https://blockstream.info/tx/push (via Tor, transaction is signed and cannot be modified)

Singlesig wallet

Multisig wallet



STATE: MULTISIG WALLET IS CREATED, SOME FUNDS ARE AVAILABLE
CAN SEND TRANSACTION 2 OF 3

Send from multisig wallet

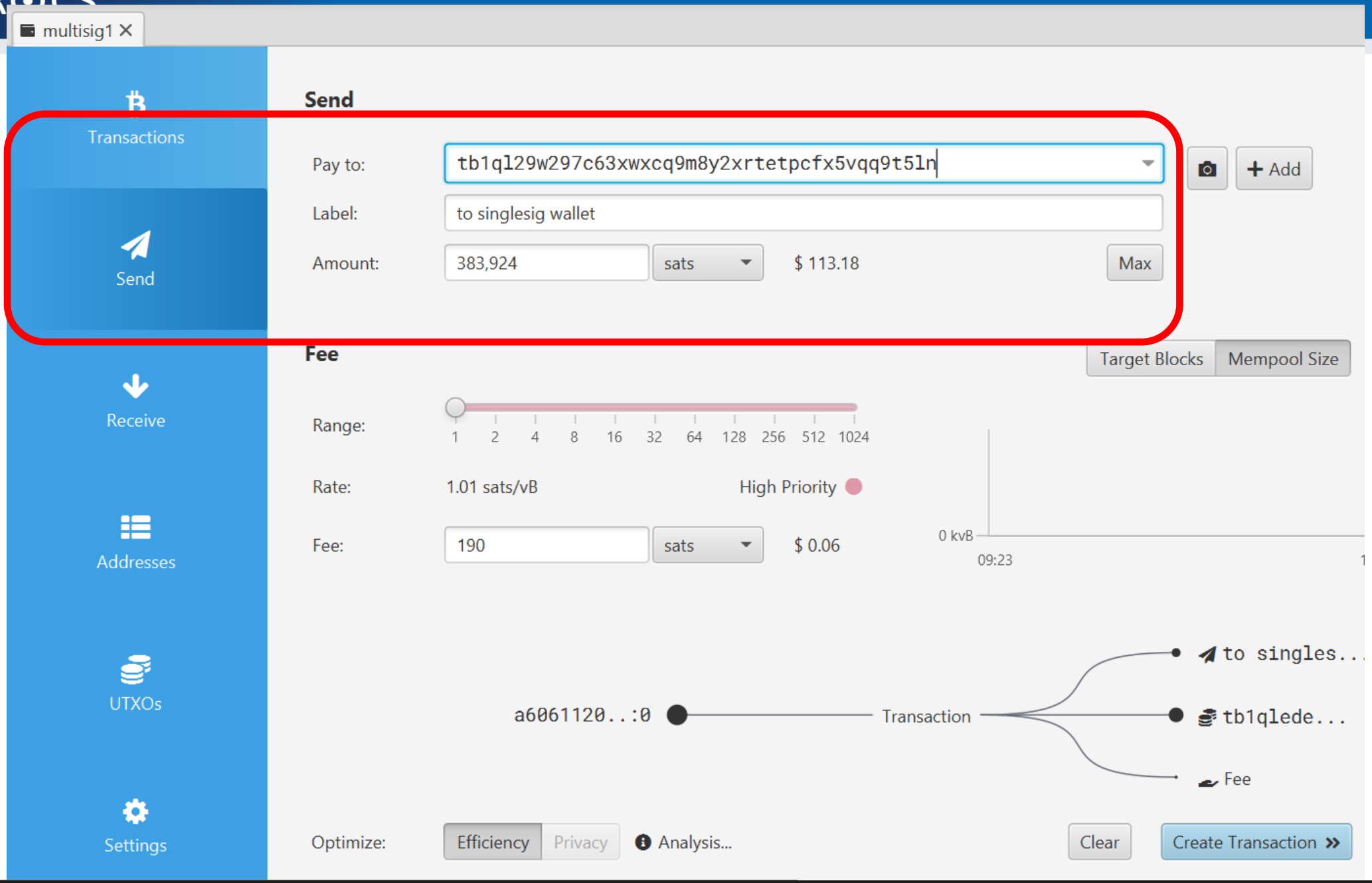
- For multisig wallet, one signature is not enough
  - Needs at least M out of N as set during wallet creation
  - Your wallet holds only one private key, group members control the rest
- Partially Signed Bitcoin Transaction (PSBT)
  - As multiple signatures must be embedded into transaction and private keys are on different computers of group members, communication must be performed
  - Partially signed transaction is passed between signers (file/QR/NFC…) until threshold M is reached (standardized format called PSBT is used)
- Every signer shall validate the transaction independently before signing
  - Is target/change address, correct? Is the amount correct?
- Anyone can broadcast resulting transaction once threshold is reached
  - Can be even broadcasted via independent service accessed via Tor (e.g., https://blockstream.info/tx/push)

Send transaction from multisig wallet (to singlesig wallet)

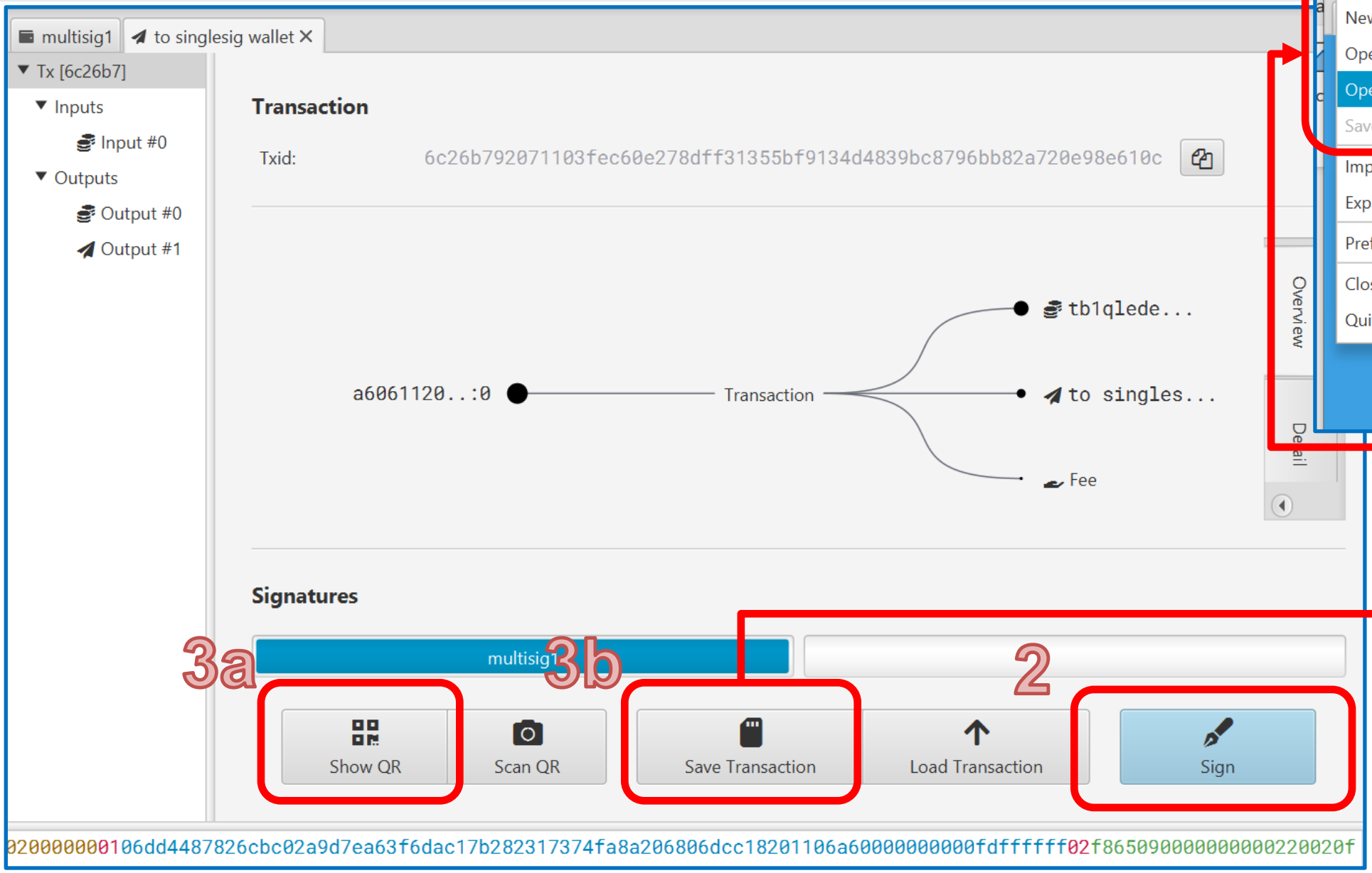
- Open any singlesig wallet (e.g., one of your group members)
  - Generate new receive address Receive→Address:

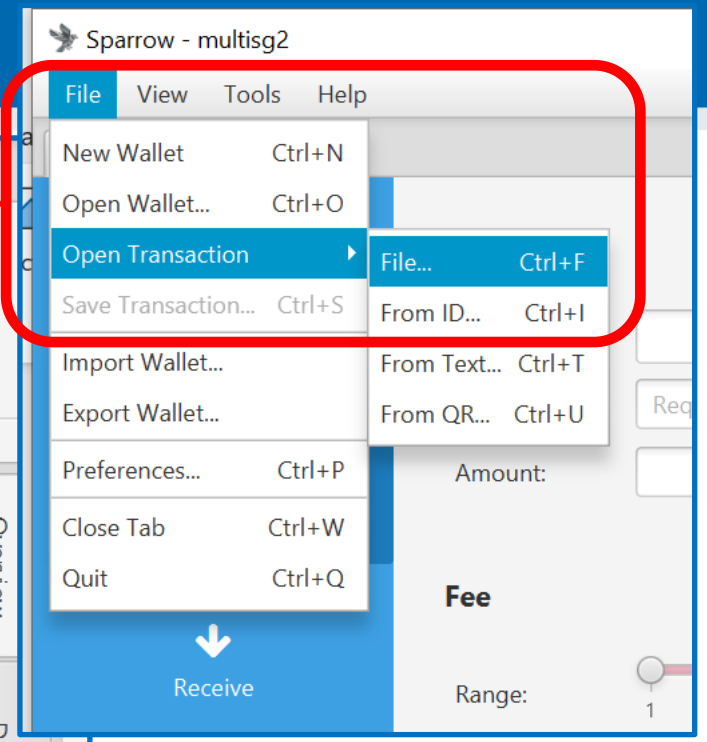
1. One member goes to his/her multisig wallet
   - Send → Pay To: paste singlesig address, set label and amount
2. Create Transaction → Finalize Transaction for Signing → Sign
   - Partially Signed Bitcoin Transaction (PSBT) is now created
3. Transfer to one of group members (PC2)
   - Option a): Show QR → variable QR displayed, scan from another machine
     4. PC2: File → Open Transaction → From QR…
   - Option b): Save Transaction → file *.psbt, load file from second machine
     4. PC2: File → Open Transaction → File…

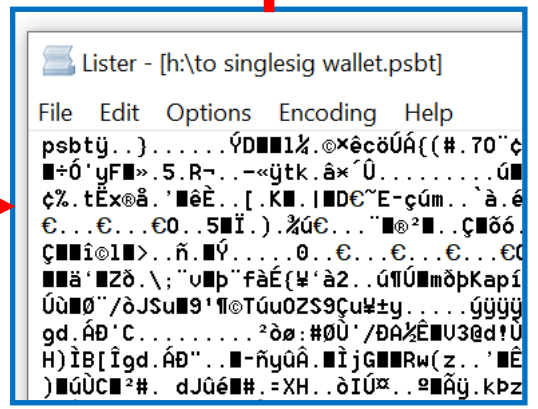
1


multisig1
Transactions
Send
Receive
Addresses
UTXOs
Settings
Send
Pay to:
tb1ql29w297c63xwxcq9m8y2xrtetpcfx5vqq9t5ln
Add
Label:
to singlesig wallet
Amount:
383,924
sats
$ 113.18
Max
Fee
Target Blocks
Mempool Size
Range:
1 2 4 8 16 32 64 128 256 512 1024
Rate:
1.01 sats/vB
High Priority
Fee:
190
sats
$ 0.06
0 kvB
09:23
a6061120..:0
Transaction
to singles...
tb1qlede...
Fee
Optimize:
Efficiency
Privacy
Analysis...
Clear
Create Transaction

4


multisig1
to singlesig wallet
Tx [6c26b7]
Inputs
Input #0
Outputs
Output #0
Output #1
Transaction
Txid:
6c26b792071103fec60e278dff31355bf9134d4839bc8796bb82a720e98e610c
a6061120..:0
Transaction
tb1qlede...
to singles...
Fee
Signatures
multisig1
3a
3b
2
Show QR
Scan QR
Save Transaction
Load Transaction
Sign
02000000010 6dd4487826cbc02a9d7ea63f6dac17b282317374fa8a206806dcc18201106a60000000000fdffffff02f8650900000000002200 20f

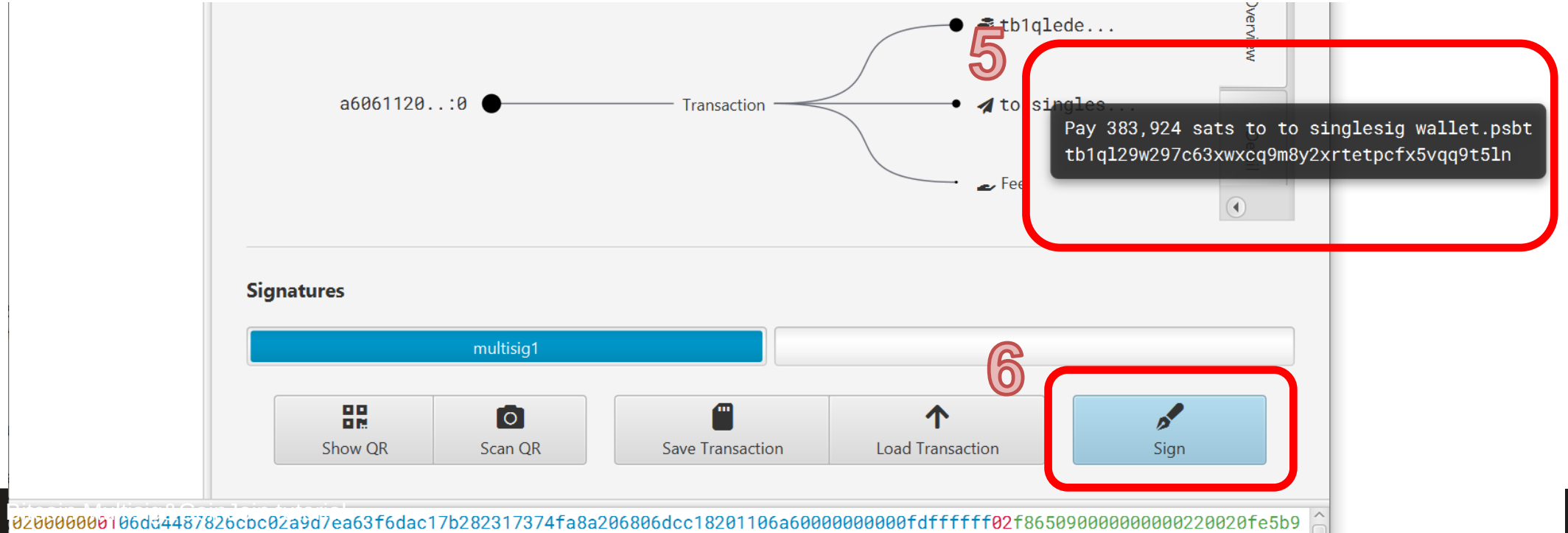

Sparrow - multisig2
File
View
Tools
Help
New Wallet Ctrl+N
Open Wallet... Ctrl+O
Open Transaction
Save Transaction... Ctrl+S
Import Wallet...
Export Wallet...
Preferences... Ctrl+P
Close Tab Ctrl+W
Quit Ctrl+Q
File... Ctrl+F
From ID... Ctrl+I
From Text... Ctrl+T
From QR... Ctrl+U
Overview
Detail
Amount:
Fee
Receive
Range:


Lister - [h:\to singlesig wallet.psbt]
File Edit Options Encoding Help
psbtÿ..}.....ÝD■■1¼.©×êcöÚÁ{(#.7O¨ç
■÷Ó'yF■».5.R¬..-«ÿtk.â×´Û.....ú■
ç%.tËx®å.'■êÈ..[.K■.|■D€˜E-çúm..`à.é
€...€...€O..5■Ï.).¾ú€...¨■®²■..Ç■õó.
Ç■■î©l■>..ñ.■Ý.....0..€...€...€...€C
■■ä'■Zð.\;¨v■þ¨fàÉ{¥'à2..ú¶Ú■mðþKapí
Úù■Ø¨/òJSu■9'¶©Túu0ZS9Çu¥±y.....ÿÿÿÿ
gd.ÁÐ'C.....²òø:#ØÙ'/ÐA½Ê■U3@d!Ù
H)ÌB[Îgd.ÁÐ"..■-ñÿûÂ.■ÌjG■■Rw(z..'■Ê
)■úÙC■²#. dJûé■#.=XH..òIÚ¤..º■Ãÿ.kÞz

Send transaction from multisig wallet (to singlesig wallet)

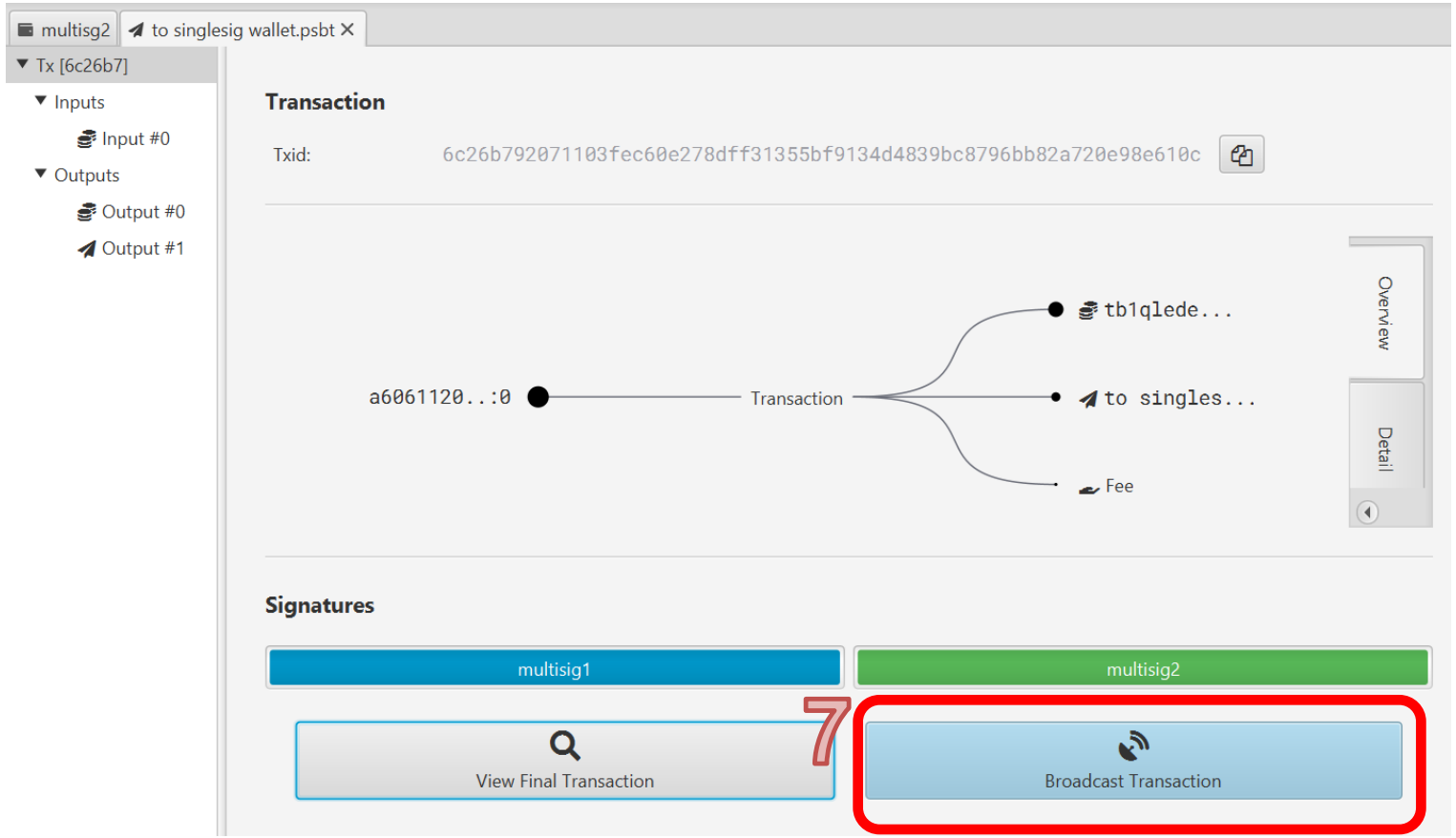
- (PSBT transaction is loaded in Sparrow wallet of second signer)

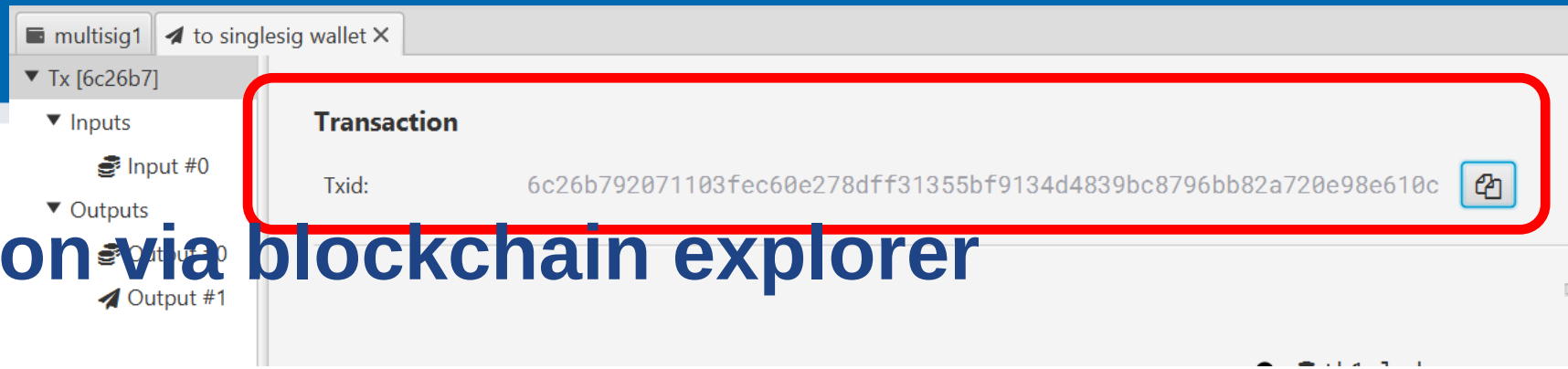
5. Check transaction parameters (address, amount, fee…)
6. If happy, click Sign button and 7. Broadcast



Send transaction from multisig wallet (to singlesig wallet)

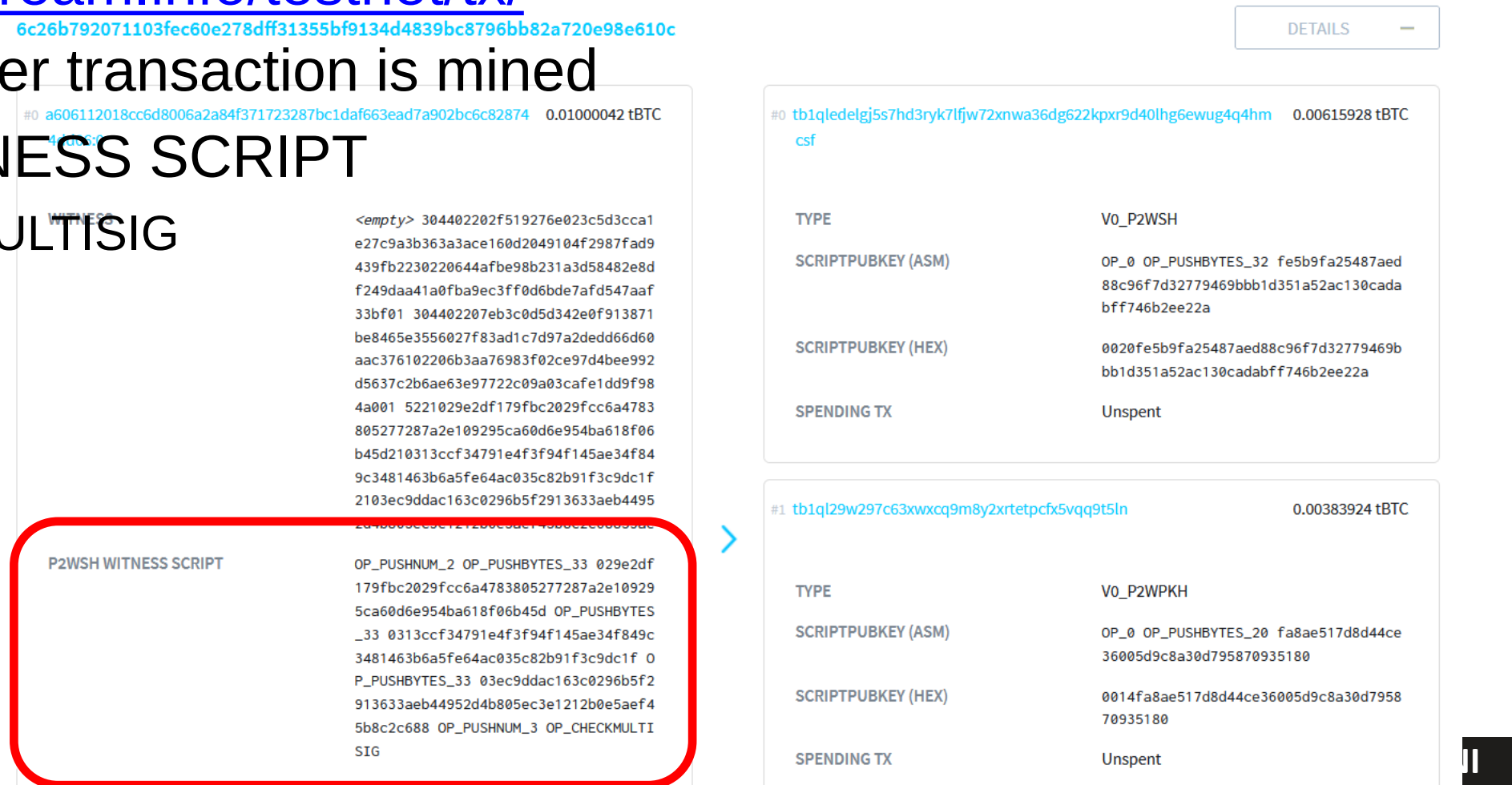
- (Signatures from multisig1 and multisig2 signers are visible)





Analyze transaction via blockchain explorer

- https://blockstream.info/testnet/tx/
- Paste Txid after transaction is mined
- P2WSH WITNESS SCRIPT
  - OP_CHECKMULTISIG



Questions

- Which option is better for backup (not loosing possibility to spend)? 1-of-3 or 3-of-3?
- Which option is better against and attacker (prevent her to spend your coins)? 1-of-3 or 3-of-3?
- What are advantages and disadvantages of 2-of-3 vs. 3-of-5?
- Can you authorize transaction of one signer not available? Two?
- Can multisig participants see all funds locked to multisig wallet?
- What shall you do if one signer loses control of funds?
- What you need to do if you would like to add another signer into quorum?
- Why is multisig transaction bigger than the singlesig one?
- Can you say if funds are locked (UTXO) to multisig wallet?
- Can you say parameters of multisig before funds are spent? After?
- Is Taproot (P2TR) changing anything?

WHIRLPOOL COINJOIN

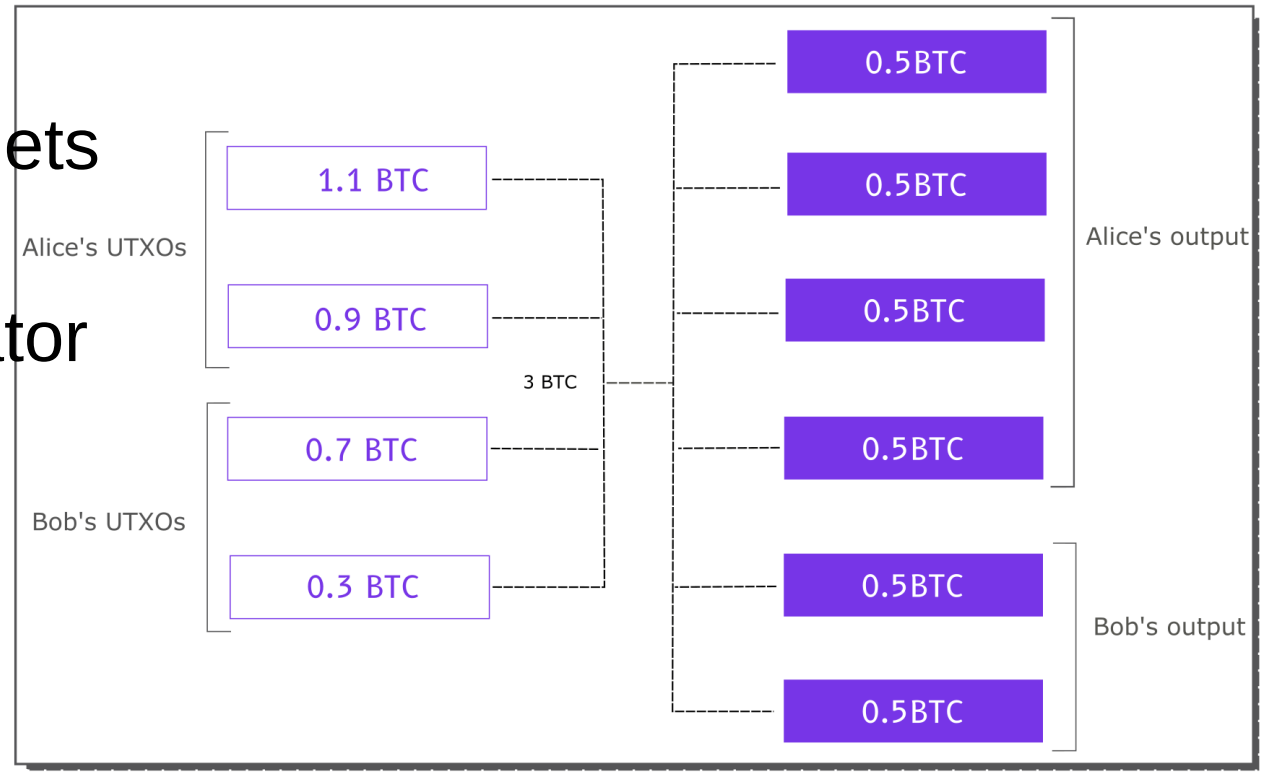
Improving privacy

- Hold your private keys (no custodial service like exchange…)
  - Cannot steal, cannot observe, cannot “vote” on your behalf
- Store private key in hardware wallet (Trezor, ColdCard, Ledger…)
  - Keys in “hot” software wallets are prone to malware attack
- Run own full node over Tor and connect your wallet to it
- Make on-chain analysis harder: https://en.bitcoin.it/wiki/Privacy
- Use manual coin selection, label coins by its origin
- Use CoinJoin, PayJoin (multiple users mix their inputs in single transaction)
- Have good opsec (no posting of own btc addresses, use Tor to broadcast tx, delink via CoinJoin after KYC…)

https://en.bitcoinwiki.org/wiki/CoinJoin
https://cryptotesters.com/blog/what-are-coinjoins-and-how-do-they-improve-bitcoin-privacy

CoinJoin

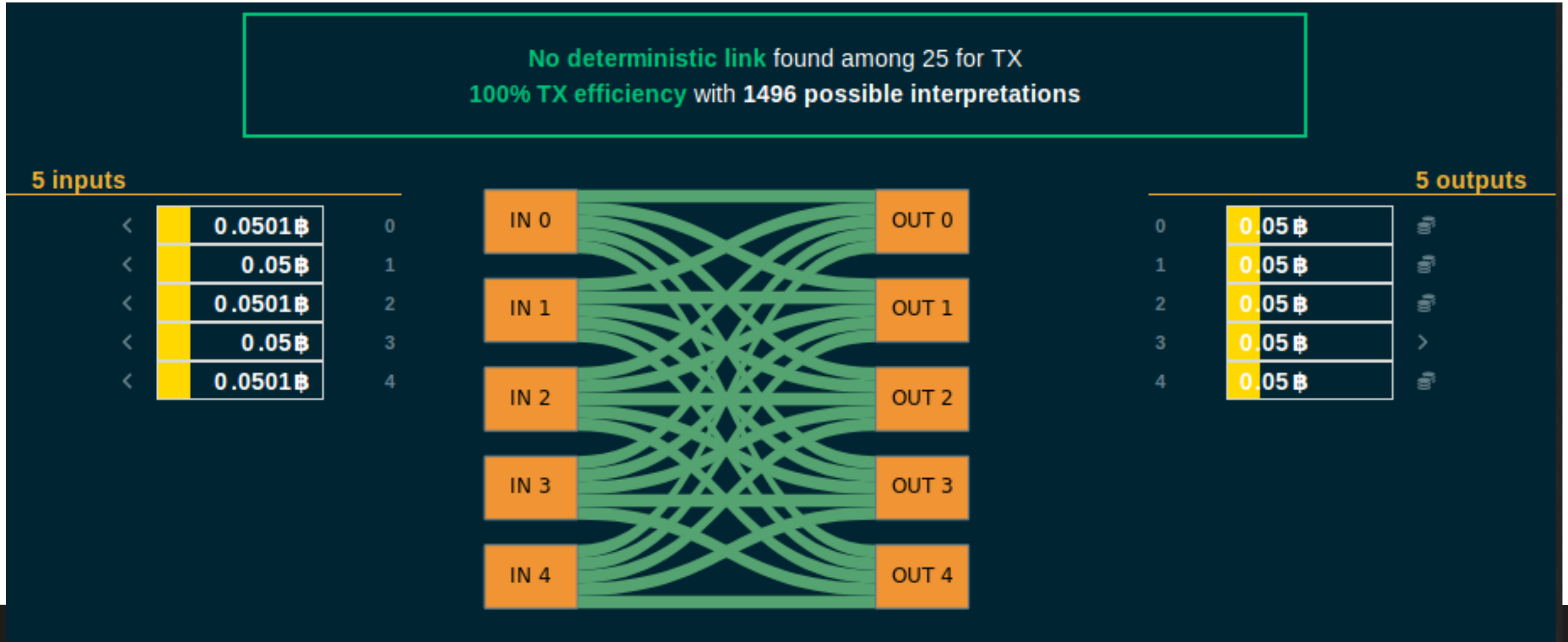
- Multiple users collaborate trustlessly in creating large transaction
- Outputs are all the same value => cannot be attributed to one of senders based on the value
- Supported by more advanced wallets
  - Wasabi, Samurai, Sparrow wallet
- Centralized, but trustless coordinator



CoinJoin implementations

- Wasabi wallet https://github.com/zkSNACKs/WalletWasabi/
  - Centralized trustless coordinator, Tor, selected number of rounds executed within hours
    - https://docs.wasabiwallet.io/using-wasabi/CoinJoin.html
  - Wasabi 2.0 (beta) will offer non-equal output coinjoin https://blog.wasabiwallet.io/privacy-guarantees-of-wasabi-wallet-2-0/
  - Anonymity set decrease over the time as people send their outputs to KYC exchanges
- Samourai Whirpool https://docs.samourai.io/en/whirlpool
  - CoinJoin with variable number of rounds, centralized trustless coordinator
  - CoinJoin runs until output is send away from Whirpool (days/months)
  - If not fullnode then xpub must be provided => privacy risk, decreased anonymity set
    - e.g., Samurai RoninDojo https://ronindojo.io/
  - Clients: Samourai wallet / Whirpool cli, SparrowWallet (using Samourai code)
- JoinMarket
  - No central coordinator, market Maker(s) run own fullnode and provide liquidity
  - Coinjoin transaction creation is coordinated by Taker who is paying also fee (on-chain and to the Maker)
  - JoininBox - JoinMarket cmdline-focused distribution https://github.com/openoms/joininbox

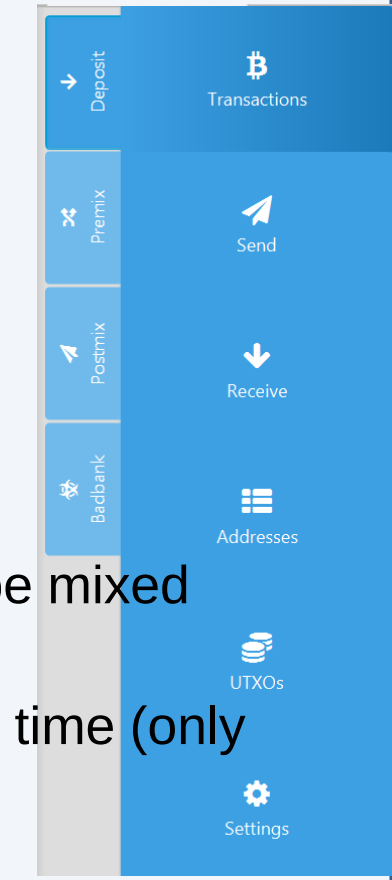
Example Whirlpool CoinJoin mixing transaction (0.05 pool)



Samourai Whirpool CoinJoin privacy mix

- CoinJoin operation is collaborative opertation with other (anonymous) users resulting in UTXOs which are harder to attribute to one user (other participants are creating anonymity set)
- Sparrow wallet contains Whirpool mix client connecting to Samourai mix coordinator executing variant of ZeroLink coinjoin protocol
  - Whirpool coordinator never holds mixed funds (untrusted)
  - All communication is done via build-in Tor (coordinator does not see your IP)
- Selected UTXOs are prepared via initial transaction called TX0 (transaction zero, Premix)
  - Registered as participant for coinjoin, fee to mix coordinator is paid
  - Smaller outputs with size almost equal to pool nominal size are created + mining fee
  - The unused change from original UTXOs is going into Badbank Change (still tied to your identity)
- As long as mixed UTXO is not send away, UTXO may be used again in future mix with other users TX0 (free additional privacy increase)
  - SparrowWallet must be running (but can be done also via Whirlpool client running on Raspberry Pi). Mixing is resumed every time SparrowWallet is online again.

Samourai Whirpool CoinJoin privacy mix



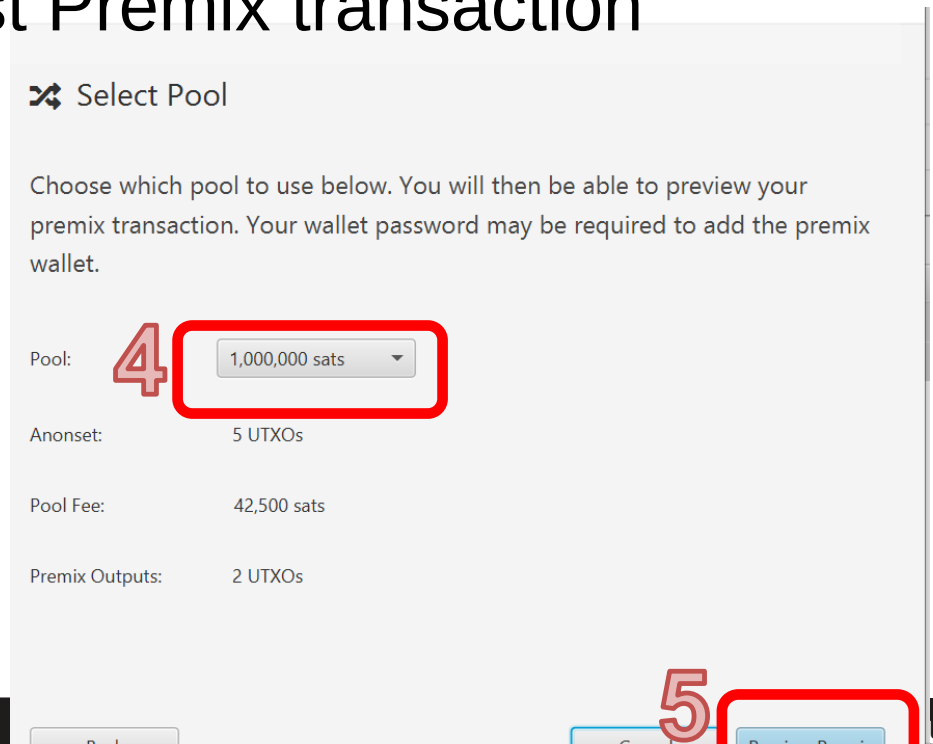
- Sparrow wallet displays funds (= your UTXOs) in different categories
  - Deposit - standard wallet funds
  - Premix – UTXOs registered for first Whirpool mix
  - Postmix – UTXOs mixed at least once (while here, are further mixed for free)
  - Badbank – UTXOs with surplus sats from TX0 when building Premix); shall not be mixed with Postmix coins (otherwise loss of privacy)
  - Categories are only indicative; all funds are still yours; you can send them at any time (only you control private keys)
- CoinJoin requires some other participants (4 in case of Whirpool)
  - on testnet, there might not be enough testing at the same time as you (but you may run 5 your instances of Sparrow wallet with different test wallets to simulate)
  - on mainnet, there are always other participants (quickly first mix you pay for, 1-2 mixes per day for subsequent free mixing)

Whirpool CoinJoin privacy mix

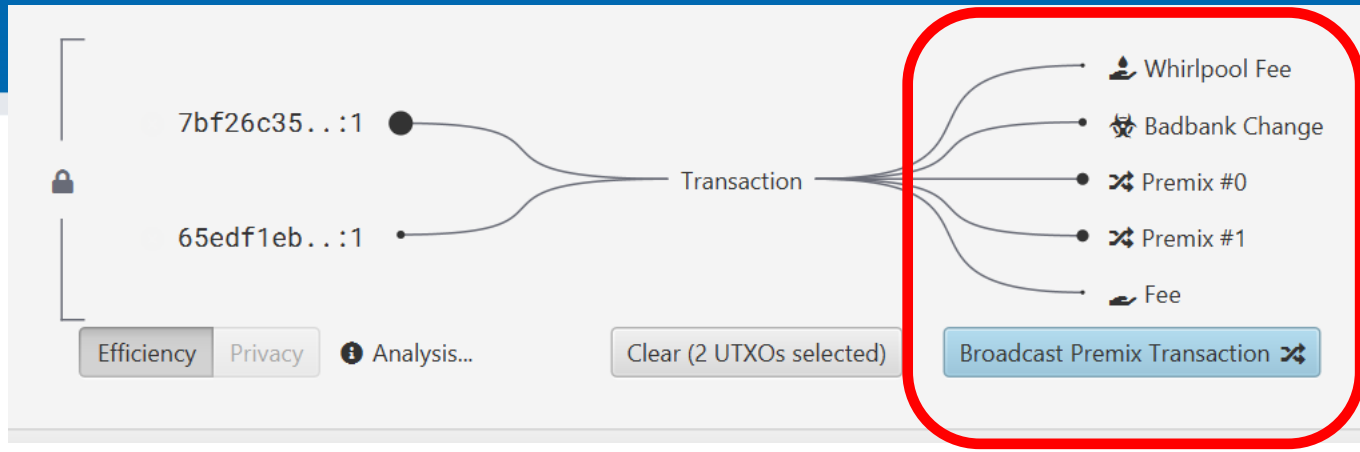
- Open your standard Sparrow single signature wallet (created before)
- Work alone – mixing participants are found automatically
  - Connection to Whirpool mixing coordinator is done via Tor
- Funds mixed are always available (you control private key)
  - can be spend them anytime

Samourai Whirlpool (CoinJoin privacy mix)

1. Click UTXO tab, 2. select one or more UTXOs
3. Click Mix Selected => Whirlpool wizard opens
4. Click Next until Select Pool, select 100k sats pool
5. Preview Premix, 6. Broadcast Premix transaction



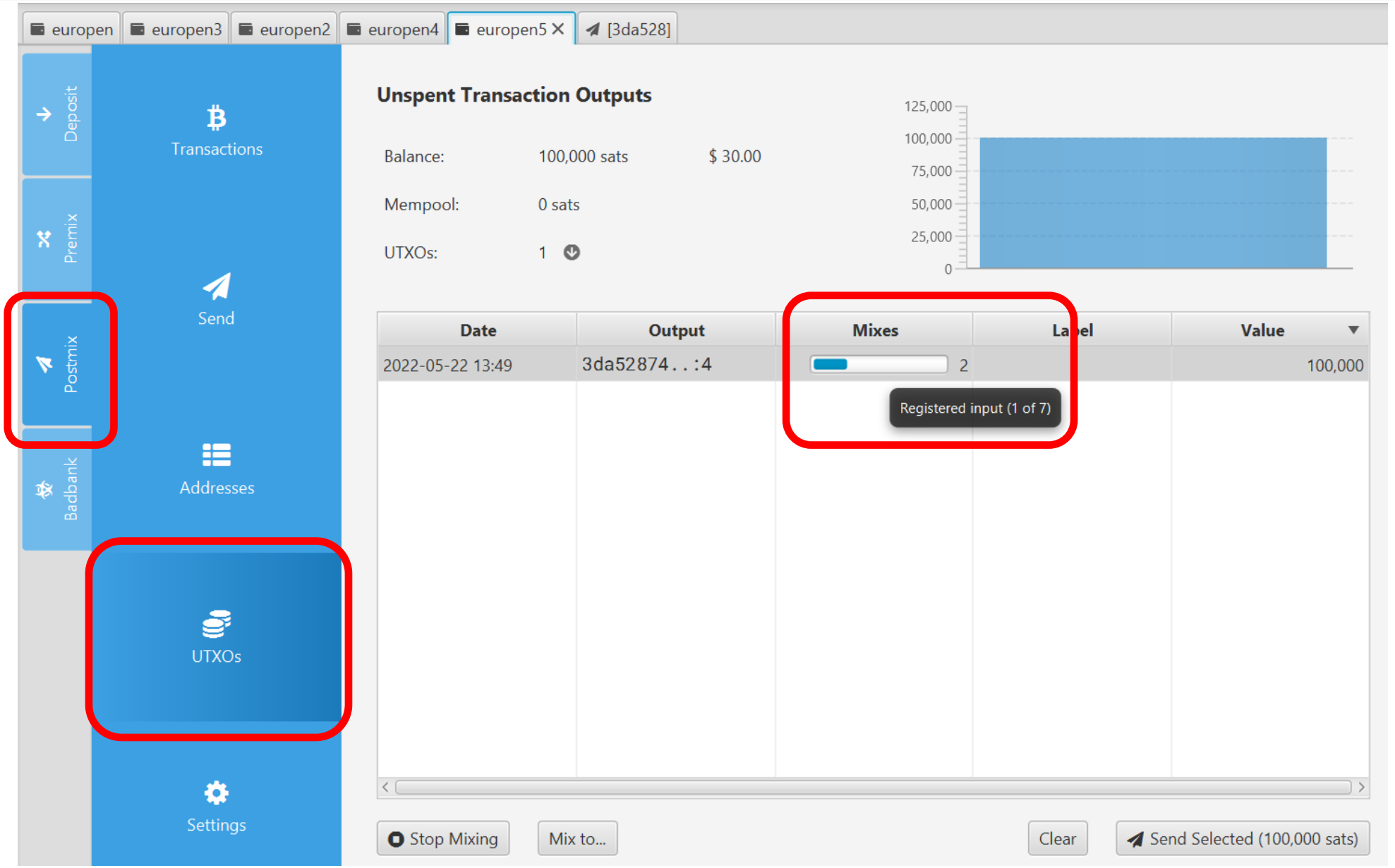
Premix transaction TX0



- Whirlpool fee – one-time payment to Whirlpool coordinator (Samourai)
  - Based on pool size, NOT amount mixed (but smaller mixed UTXOs as result)
- Fee – mining fee to miners (based on actual blockspace demand)
- Premix #0, #1 … #N – initial premixed inputs of same size
  - These UTXOs will be input to mixing rounds
- Badbank change – remaining sats which cannot be put into another Premix #N+1 (as is smaller than mixing pool minimal size)
  - “toxic waste” – this UTXO is still tied to original input transaction (~your identity)
  - Do not merge with any mixed outputs (deanonimized)

Mixing procedure

- When TX0 is send to mempool, new UTXO(s) display in Premix tab
  - Wait till TX0 is confirmed, multiple UTXOs created based on the pool size and mixed amount
- Automatically, new Whirpool mixing transaction is created
  - New UTXO is displayed in Postmix tab
- As new blocks are mined, Postmix UTXOs are automatically included in subsequent mixing transaction(s) – Mixes column
  - Mixed unless wallet user send them elsewhere (continuous increase of anonymity set)
  - Mixed when someone creates new TX0 (new UTXO is paying for mining fees)
- Sparrow wallet must run for active mixing
  - Mixing is resumed automatically if Sparrow wallet is started again
- Funds can be spent anytime, options with improved privacy, send to another wallet after defined number of mixes…


europen
europen3
europen2
europen4
europen5
[3da528]
Deposit
Premix
Postmix
Badbank
Transactions
Send
Addresses
UTXOs
Settings
Unspent Transaction Outputs
Balance: 100,000 sats $ 30.00
Mempool: 0 sats
UTXOs: 1
125,000
100,000
75,000
50,000
25,000
0
Date
Output
Mixes
Label
Value
2022-05-22 13:49
3da52874..:4
2
100,000
Registered input (1 of 7)
Stop Mixing
Mix to...
Clear
Send Selected (100,000 sats)

Analyze mixing transaction

1. Analyze using Sparrow wallet visualization
   – UTXO, symbol of magnifier , click topmost item Tx […]
2. Analyze using blockchain explorer
   – Copy txid, use https://blockstream.info/testnet/tx/

- For mainnet transactions, other privacy estimation tools exist
  – Always use Tor when accessing! (do not link your IP with transactions of interest)
  – https://KYCP.org (single transaction, examples)
  – https://oxt.me (graph of transactions, forensic analysis)

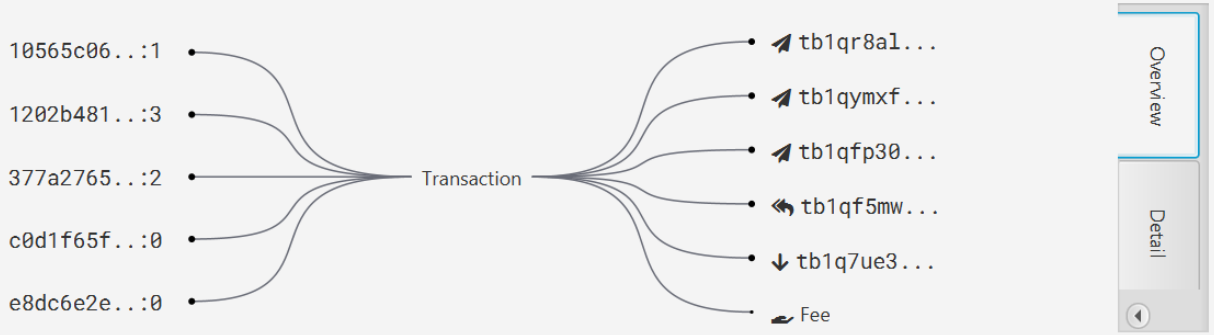
1

europen | europen3 | europen2 | europen4 | europen5 | [3da528] ×

- Tx [3da528]
  - Inputs
    - Input #0
    - Input #1
    - Input #2
    - Input #3
    - Input #4
  - Outputs
    - Output #0
    - Output #1
    - Output #2
    - Output #3
    - Output #4

Transaction

Txid: 3da52874471746d2fec8f6c246392a5274a21d4fe557f435c5bb76d39a0f3e77



Blockchain

Status: 3 Confirmatio

Block Height: 2226930

Timestamp: 2022-05-22 1

Block Hash: 000000000

PRIVACY ANALYSIS

2 Possibly a CoinJoin transaction

3da52874471746d2fec8f6c246392a5274a21d4fe557f435c5bb76d39a0f3e77

DETAILS +

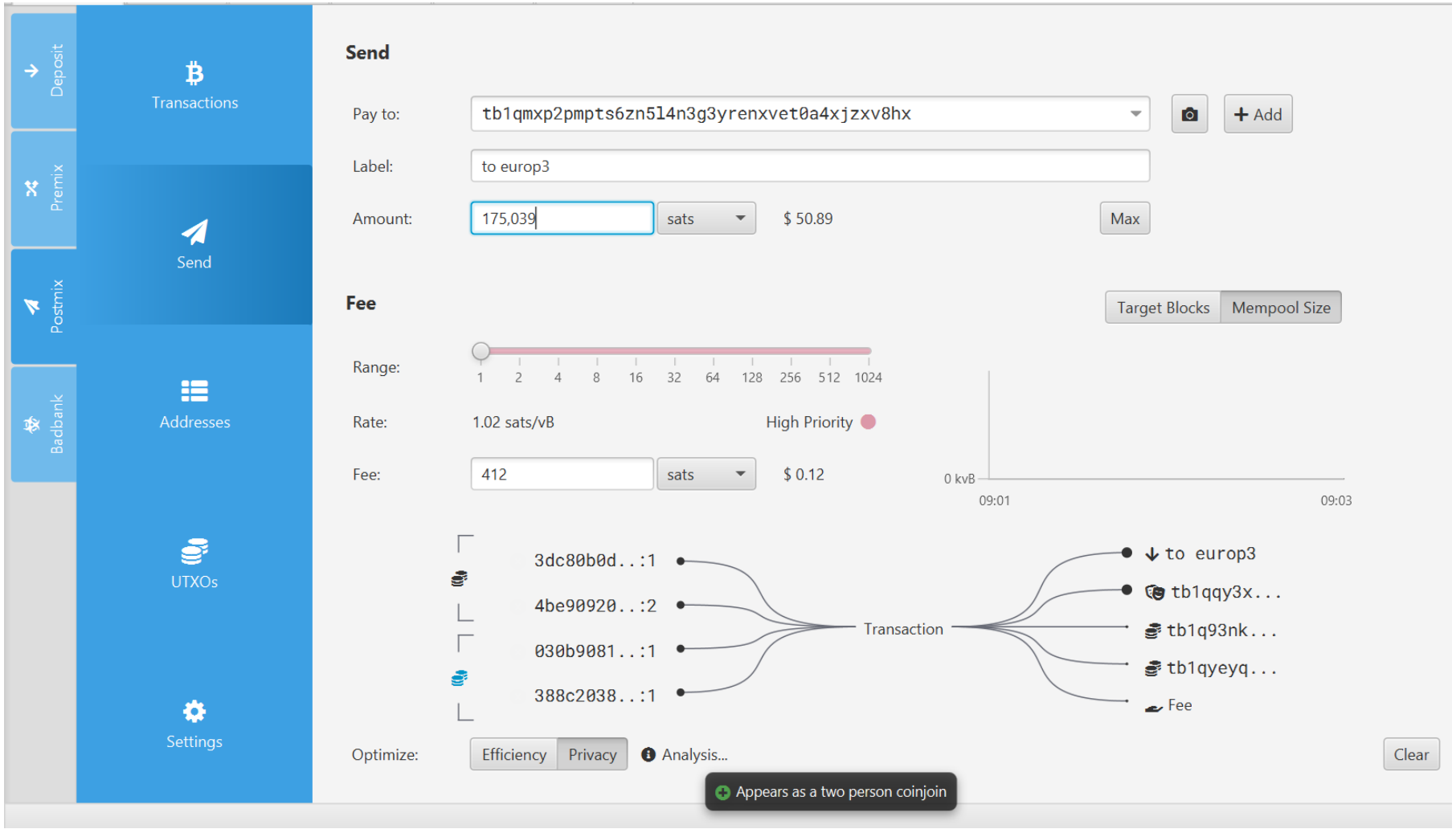
#0	10565c0673127c469c20c09ba794fbf037829bae501c55e6b92257e850b96c52:1	0.001 tBTC
#1	1202b4818529834229e49c3cca7df364536b0f7baa6f080795536ee70f8d15d8:3	0.00100302 tBTC
#2	377a2765e7ef45ffed10f0f3c5f573ebd753d1a2313abddb24e652de6b836ba1:2	0.00100302 tBTC
#3	c0d1f65ff9082972a33ba81f2ad93f82d7fcd37391185e7b1aa70242d89d5c01:0	0.001 tBTC

#0	tb1qr8al4cc0s5zu2pyqqrzdts243sr7k9hmc80ket	0.001 tBTC
#1	tb1qymxfyvf37gr3ztst8p8dj5cmwr48w7rda72glg	0.001 tBTC
#2	tb1qfp309nz0l0fd2zqaa2s3lr9prykmw08tpe9chc	0.001 tBTC
#3	tb1qf5mwxawpcj8hraz5nd6e2u9s388n0a5xpjwmrf	0.001 tBTC
#4	tb1q7ue3sy6rjmzdadz9t8wzaqc98ev5kqcsyvfmau	0.001 tBTC

Post-mix spending

- CoinJoin mixing breaks on-chain heuristics (input→output)
- Your UTXO is now private, but must be also used privately later
- Do not use mixed (Postmix) and unmixed (Badbank) UTXOs!
- Fake/real collaborative spent (PayJoin)
  - Two or more people spending together (inputs from both, outputs to both)
  - Simulated PayJoin (all inputs yours, but looks like collaborative spent)
- Coin control
  - Whole UTXO send to new address (no change)
- Atomic swap – trustless exchange of UTXOs (even on different chains)
  - Utilizes timelock – transaction must be finished by both parties till deadline, otherwise cancel

Postmix spent – simulated PayJoin

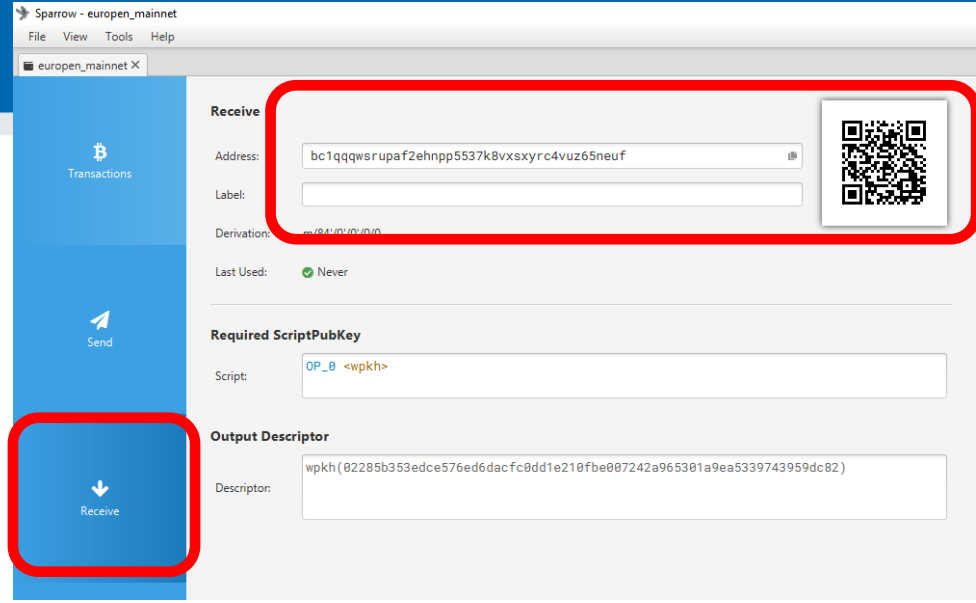


Questions

- Does Whirpool CoinJoin require online connectivity?
- How many other participants are required?
- How many mixing rounds are enough?
- What is the difference between mixing pools?
- Who is paying for the mixing transaction?
- What happens if you create transaction using both Postmix UTXO and Badbank UTXO?

PLAYING WITH REAL BTC

Receive real btc



- Run Sparrow on mainnet (not testnet)
  - Omit `-n testnet` switch
- Create new wallet, make sure 12 words are written securely on paper
- Prepare new receive address (shall start with bc1…)
  - Show QR code, wait till we send some sats to you
- Things to try: send to mobile wallet, coinjoin with collegues, Lightning…
- Keep in mind:
  - Do not loose the paper backup, this is for real ☺
  - Every send costs you small fee (set only 1sat/vB, Mempool clears frequently)
  - Have fun!

FEEDBACK

Thank you, please give us feedback

- We hope you liked the tutorial
- Please provide any feedback either in person
  - Or write into slido.com
- Always happy to chat with beer!

Checkout

- Which of the seminar parts you enjoyed most?
- Rank it according the level of enjoyment (most interesting => first)
- Write to sli.do when displayed

slido

Which part of the tutorial you liked most?

ⓘ Start presenting to display the poll results on this slide.

slido

Audience Q&A Session

ⓘ Start presenting to display the audience questions on this slide.