PV204 Security technologies

Cryptocurrencies II. - Bitcoin multisig, CoinJoin, PayJoin

Petr Švenda *svenda@fi.muni.cz* *@rngsec*

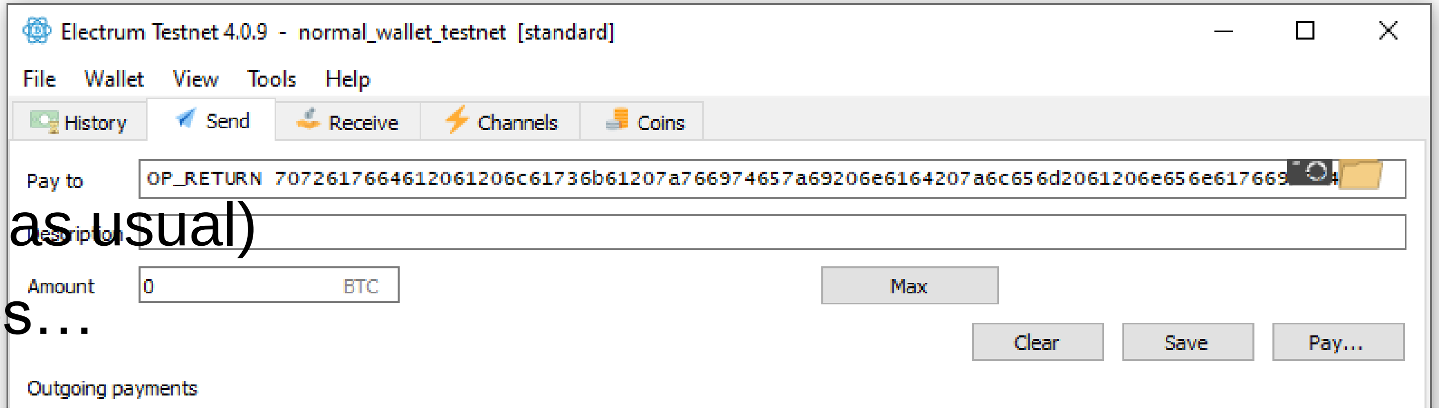
Centre for Research on Cryptography and Security, Masaryk University

Centre for Research on
Cryptography and Security

OP_RETURN

Task: Store custom (limited) data into blockchain

- OP_RETURN instruction in lock script for provably non-spendable tx
  - – Script execution never TRUE, full nodes can drop from list of UTXOs
- Send via Electrum
  - – OP_RETURN data (in hexa)
  - – 0 amount (sender pays tx fees as usual)
  - – 40 bytes, usable for timestamps…



Electrum Testnet 4.0.9 - normal_wallet_testnet [standard]

Pay to: OP_RETURN 7072617664612061206c61736b61207a766974657a69206e6164207a6c656d2061206e656e617669

Description:

Amount: 0 BTC

- Locate tx on blockchain
  - – https://blockstream.info/testnet/
- With 1 peer: Find three ideas what to include and why
  - – What information, how encoded, how retrieved, what security benefits

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

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

Single signature

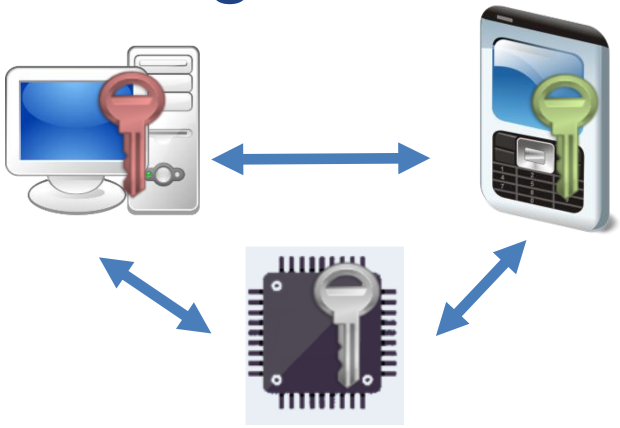
Signature

Yosemite Faculty Association
Student Senate
Leadership Team Advisory Council
California School Employees Association
College Council
Academic Senate

Multiple signatures

Signature Signature Signature

MPC signature



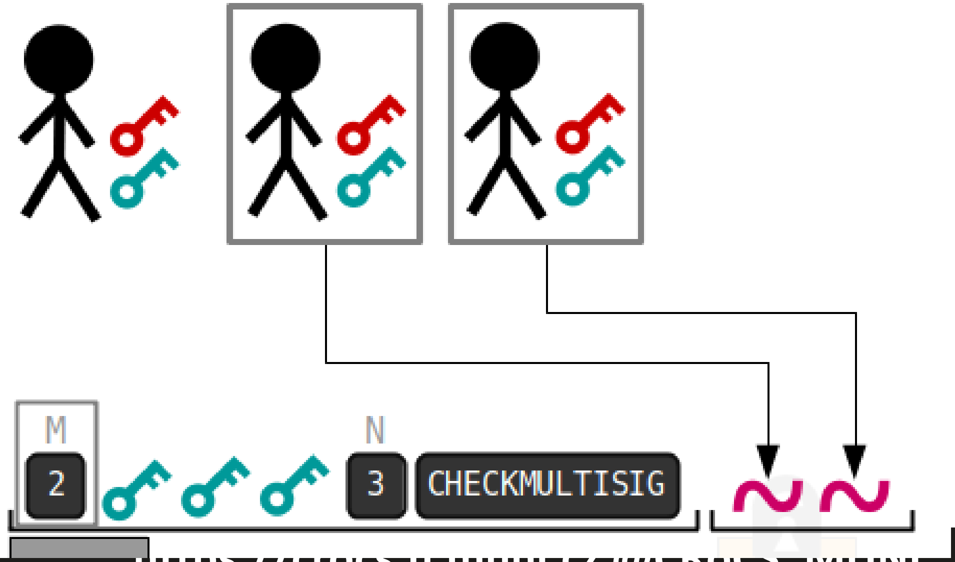
Signature

1. Shamir 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

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 k-out-of-n, https://en.bitcoin.it/wiki/Multisignature
- P2MS, P2MS wrapped in P2SH
  - – https://learnmeabitcoin.com/technical/p2ms

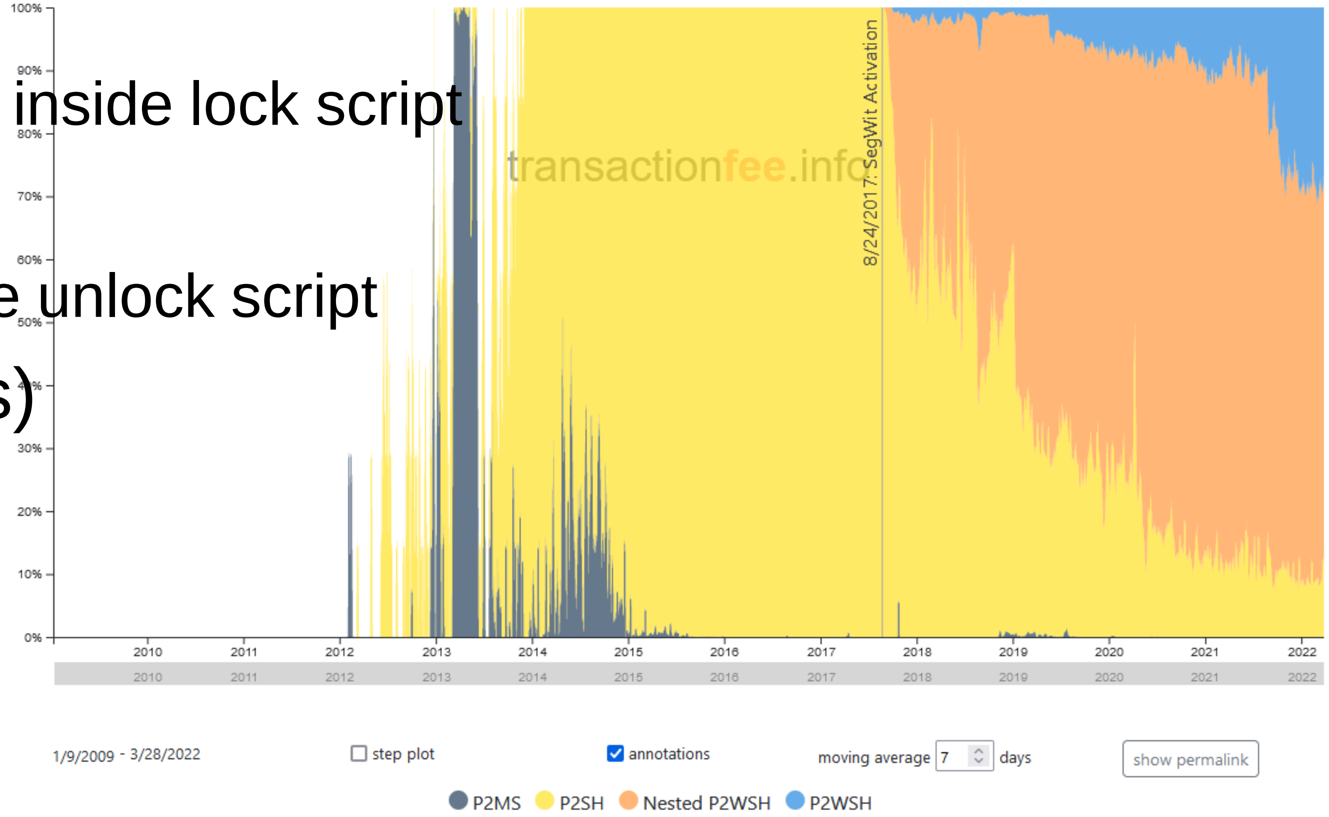


3. Secure multi-party computation (MPC)

- 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
- 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
- Can tell for P2MS
  - Threshold and allowed public keys inside lock script
- Can tell for P2SH (if spent)
  - Multisig script and used keys inside unlock script
- (analogically for Segwit variants)



1/9/2009 - 3/28/2022

□ step plot

☑ annotations

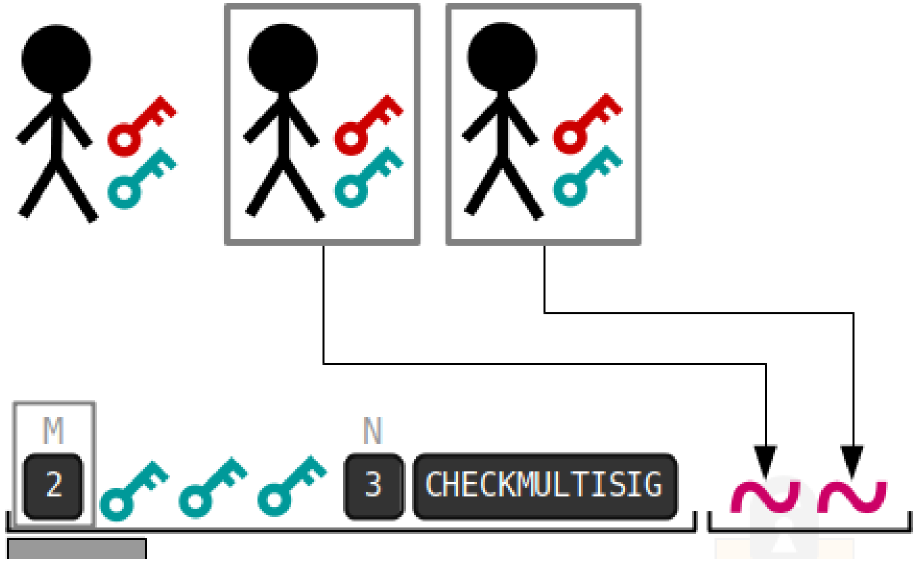
moving average 7 days

show permalink

MULTISIGNATURES

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 k-out-of-n, https://en.bitcoin.it/wiki/Multisignature
- P2MS, P2MS wrapped in P2SH
  - https://learnmeabitcoin.com/technical/p2ms
- Today, we will use P2SH and k-out-of-n



Task: using multisignature wallet (3ppl/room)

1. Create new 2-out-of-3 multisignature wallet in Electrum
   – All three people in the group are participants (separate machines)
2. Send some coins from last week to multisig wallet
   – Generate new receiving address
   – Wait till included in block

- Analyze TX (from normal to multisig) via chain explorer - How lock script looks like? Why?
  – Screenshot explorer, annotate

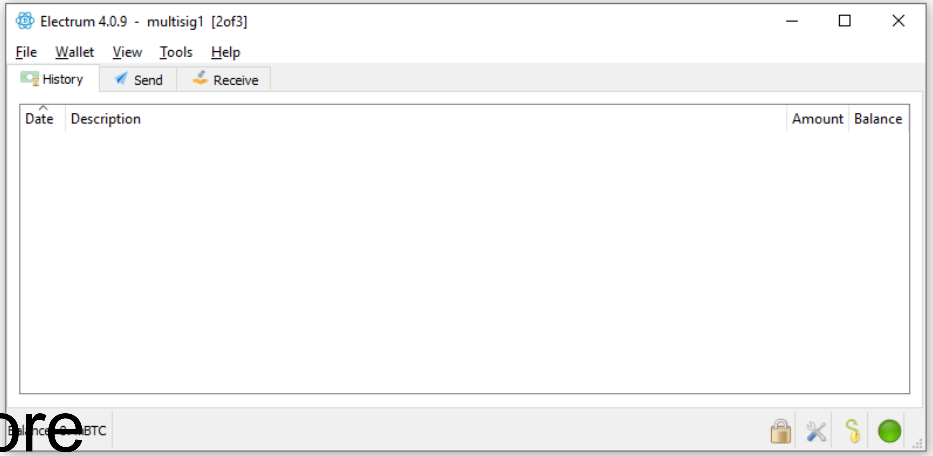
3. Send from multisig wallet back to standard one
   – Why you need to generate PSBT?
   – Is it safe to send PSBT via email?
   – Who can broadcast transaction when 1, 2 and 3 signatures are made?

- Analyze TX (from multisig to normal) via chain explorer - How unlock script looks like? Why?
  – Screenshot explorer, annotate

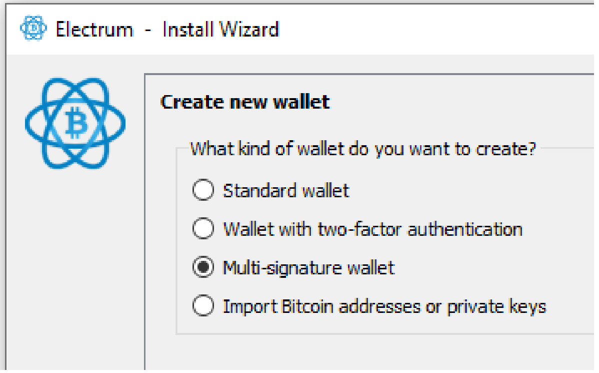
Important: Use Electrum 4.2.0 or higher

- You need to have same type of address
  - 4.2.0 is allowing only for segwit addresses
  - Older version may allow for legacy addresses – can’t be mixed with segwit

Creating multisig wallet (--testnet)



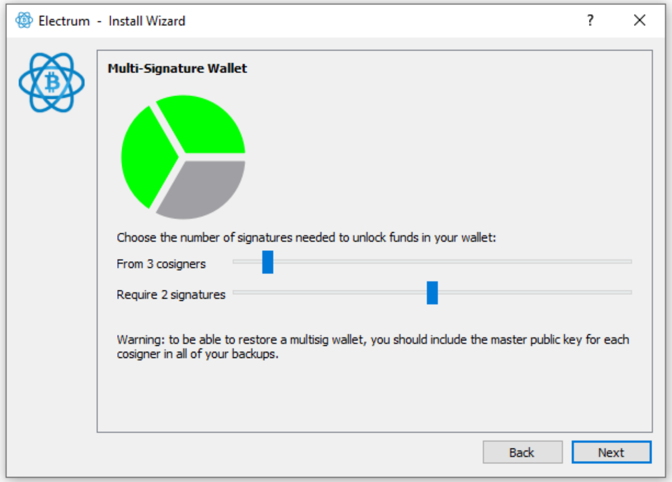
- If you already have wallet: File → New/Restore
  - All three people performs the same process
- Save seed and masterpub key for yourself (cosigner 1)
- Get masterpub key from others, Add cosigner (2 of 3), (3 of 3)
- Finish creation of multisig wallet



Create new wallet

What kind of wallet do you want to create?

○ Standard wallet
○ Wallet with two-factor authentication
● Multi-signature wallet
○ Import Bitcoin addresses or private keys



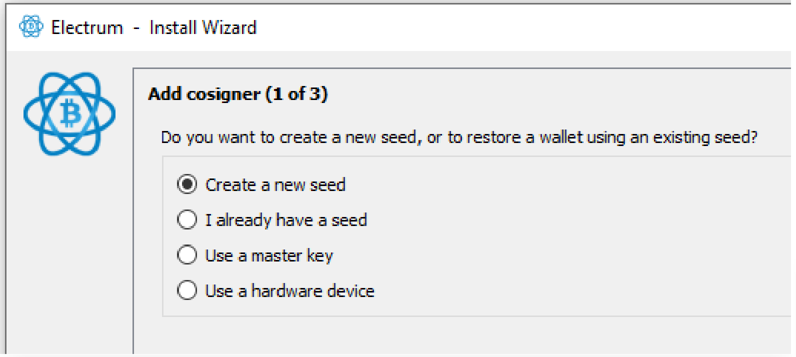
Multi-Signature Wallet

Choose the number of signatures needed to unlock funds in your wallet:

From 3 cosigners

Require 2 signatures

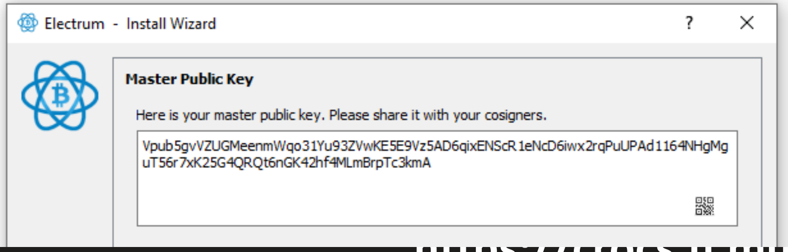
Warning: to be able to restore a multisig wallet, you should include the master public key for each cosigner in all of your backups.



Add cosigner (1 of 3)

Do you want to create a new seed, or to restore a wallet using an existing seed?

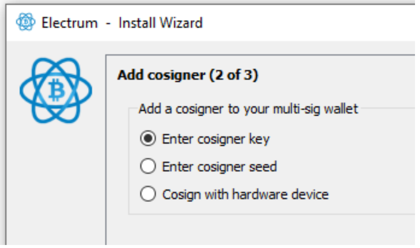
● Create a new seed
○ I already have a seed
○ Use a master key
○ Use a hardware device



Master Public Key

Here is your master public key. Please share it with your cosigners.

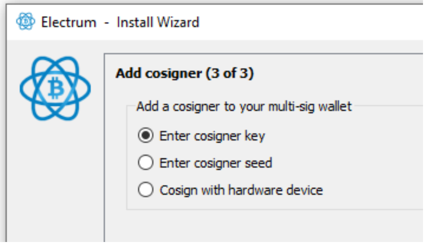
```
Vpub5gvVZUGMeenmWqo31Yu93ZVwKE5E9Vz5AD6qixENScR1eNcD6iwx2rqPuUPAd1164NHgMg
uT56r7xK25G4QRQt6nGK42hf4MLmBrpTc3kmA
```



Add cosigner (2 of 3)

Add a cosigner to your multi-sig wallet

● Enter cosigner key
○ Enter cosigner seed
○ Cosign with hardware device



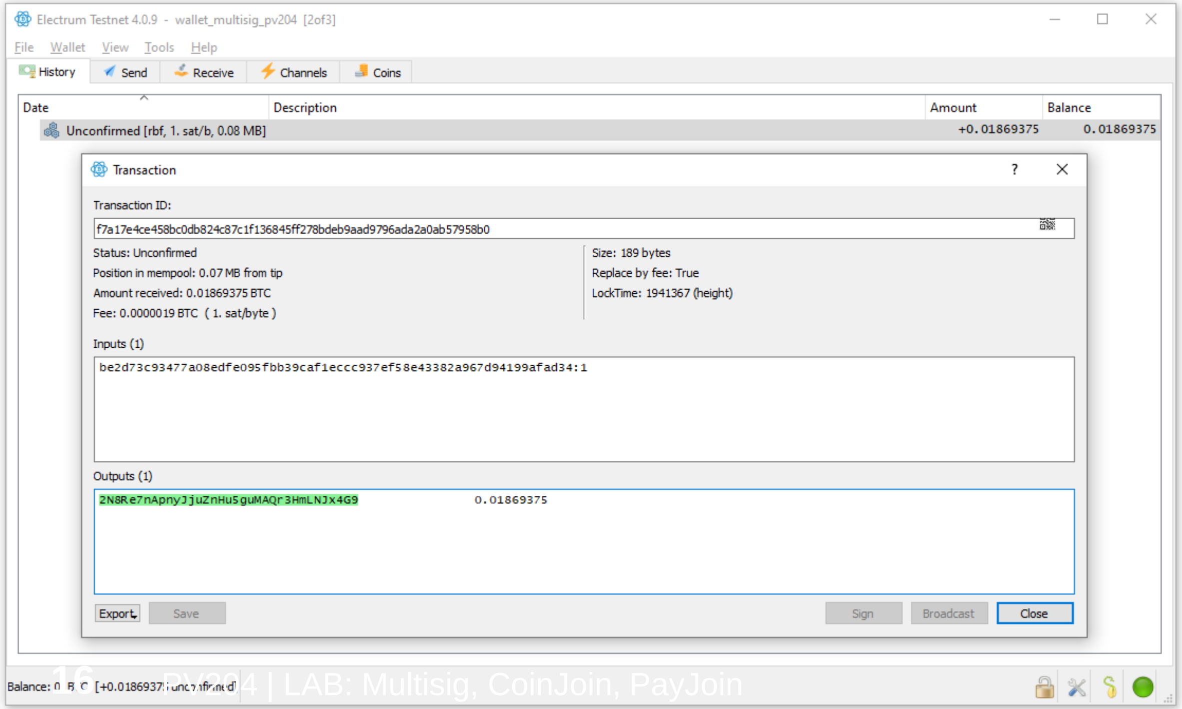
Add cosigner (3 of 3)

Add a cosigner to your multi-sig wallet

● Enter cosigner key
○ Enter cosigner seed
○ Cosign with hardware device

Send from normal wallet to multisig one

- Generate receive address on multisig, send to it from normal one
- Optional: try using coin control
  - View → Show coins, RClick on target coin → Spend
  - Max button in Send will only take marked coin(s)


Electrum Testnet 4.0.9 - wallet_multisig_pv204 [2of3]
File Wallet View Tools Help
History Send Receive Channels Coins
Export Save
Sign Broadcast Close

Date	Description	Amount	Balance
Unconfirmed [rbf, 1. sat/b, 0.08 MB]		+0.01869375	0.01869375

Transaction

Transaction ID:

```
f7a17e4ce458bc0db824c87c1f136845ff278bdeb9aad9796ada2a0ab57958b0
```

Status: Unconfirmed
Position in mempool: 0.07 MB from tip
Amount received: 0.01869375 BTC
Fee: 0.0000019 BTC (1. sat/byte)

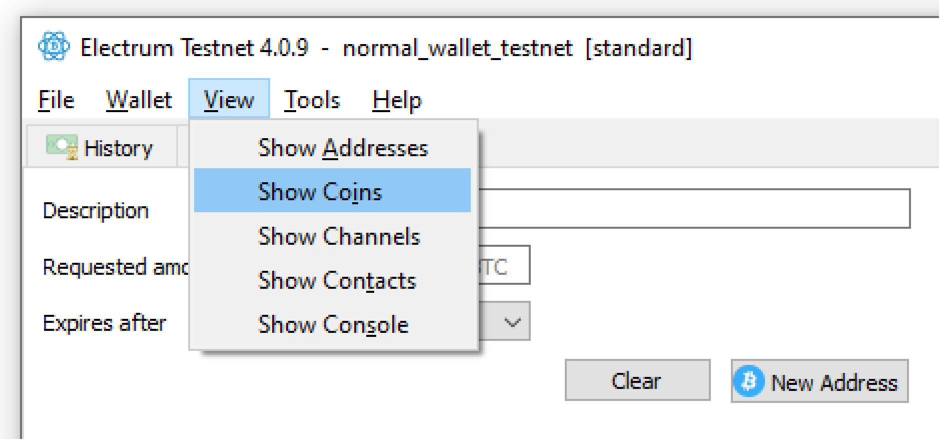
Size: 189 bytes
Replace by fee: True
LockTime: 1941367 (height)

Inputs (1)

```
be2d73c93477a08edfe095fbb39caf1eccc937ef58e43382a967d94199afad34:1
```

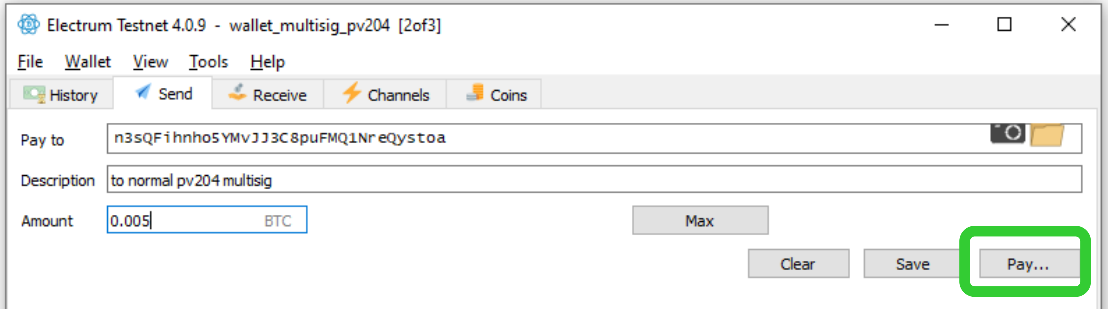
Outputs (1)

```
2N8Re7nApnyJjuZnHu5guMAQr3HmLNJx4G9          0.01869375
```



Send from multisig wallet to normal one – first signer

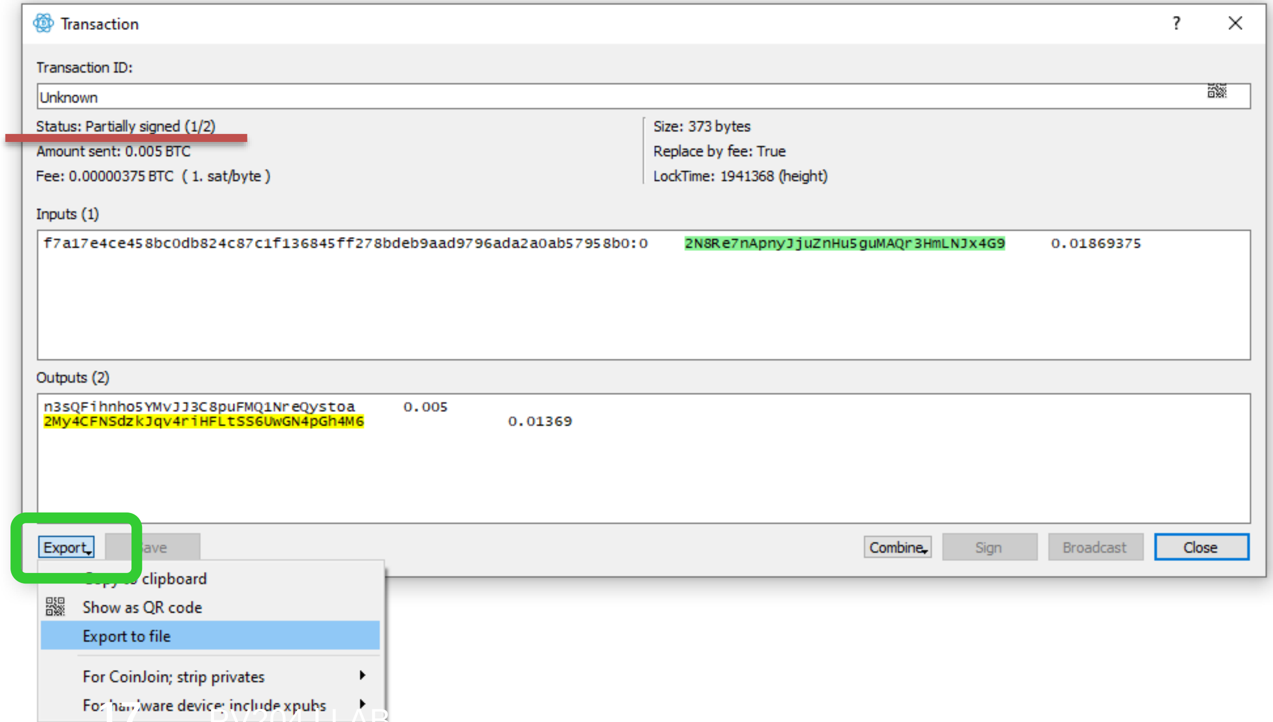
- Generate receive address on normal wallet
- One signer creates transaction
  - Save button saves partially prepared tx locally
  - Pay button signs (partially) transaction, allows to Export



Pay to: n3sQFihnho5YMvJJ3C8puFMQ1NreQystoa

Description: to normal pv204 multisig

Amount: 0.005 BTC



Transaction ID:
Unknown

Status: Partially signed (1/2)
Amount sent: 0.005 BTC
Fee: 0.00000375 BTC (1. sat/byte)

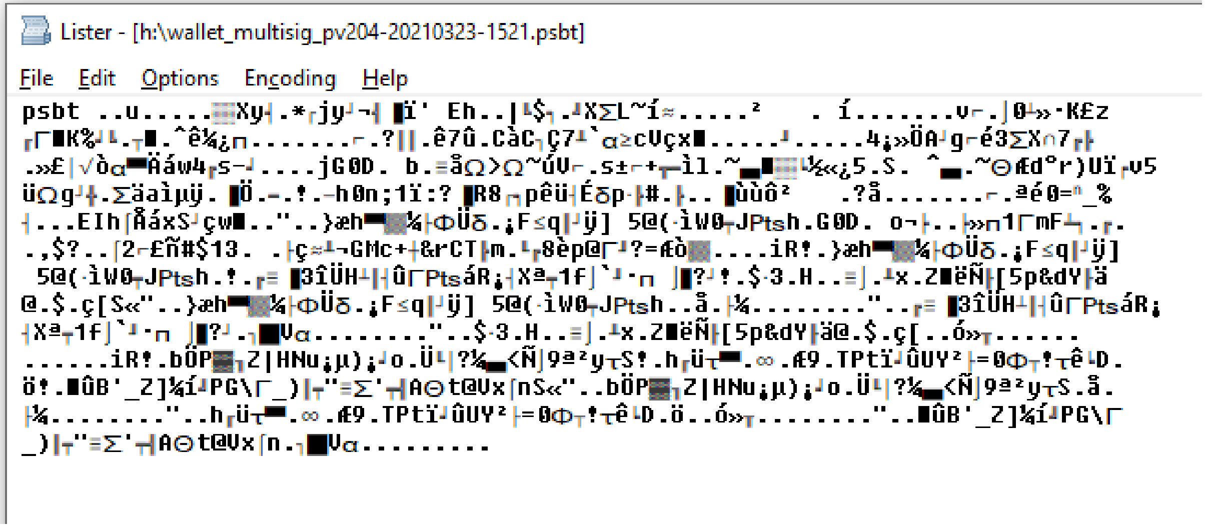
Size: 373 bytes
Replace by fee: True
LockTime: 1941368 (height)

Inputs (1)

```
f7a17e4ce458bc0db824c87c1f136845ff278bdeb9aad9796ada2a0ab57958b0:0     2N8Re7nApnyJjuZnHu5guMAQr3HmLNJx4G9     0.01869375
```

Outputs (2)

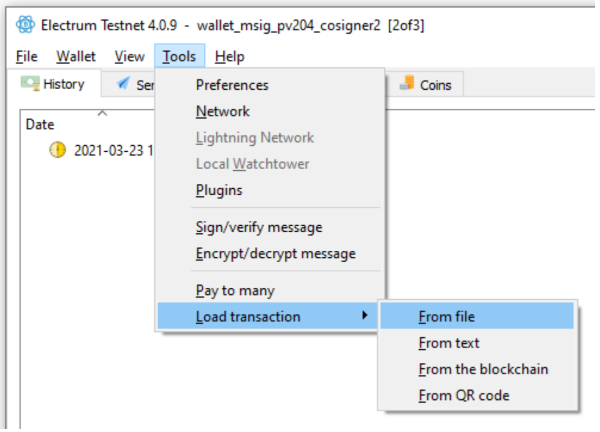
```
n3sQFihnho5YMvJJ3C8puFMQ1NreQystoa      0.005
2My4CFNSdzkJqv4riHFLtSS6UwGN4pGh4M6              0.01369
```

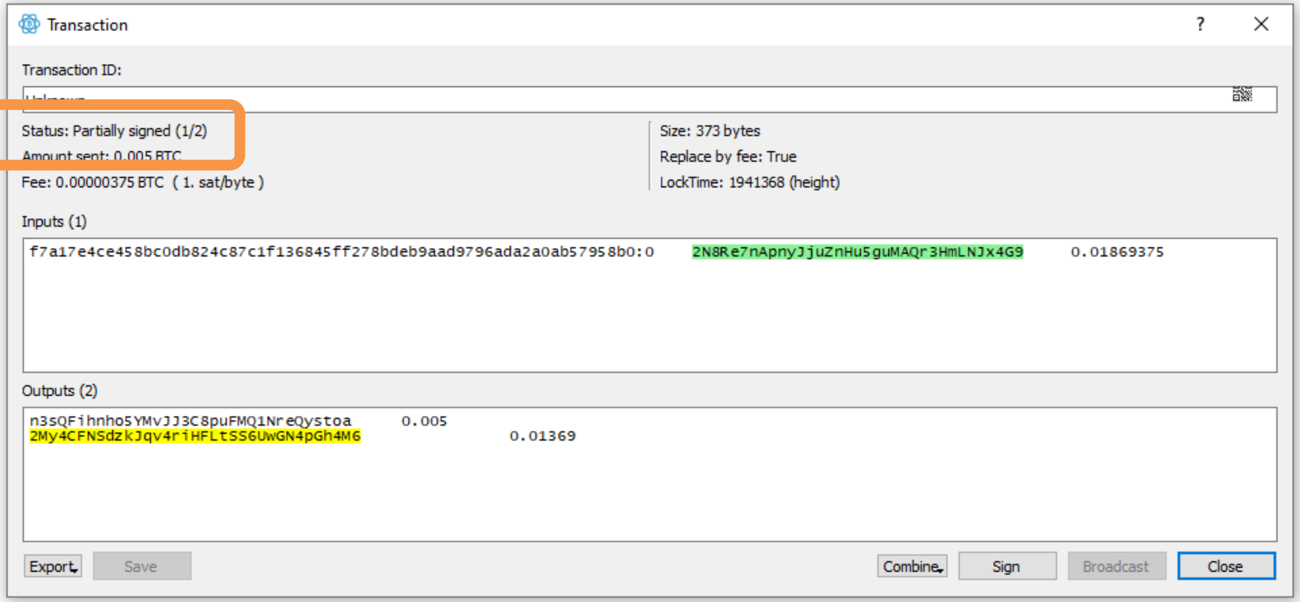


```
psbt
```

Send from multisig wallet to normal one – second signer

- Open cosigner’s wallet
- Tools→Load transaction→From file
- Check target info and amount
- Sign loaded transaction
- Broadcast to network





Transaction ID:
Unknown

Status: Partially signed (1/2)
Amount sent: 0.005 BTC
Fee: 0.00000375 BTC (1. sat/byte)

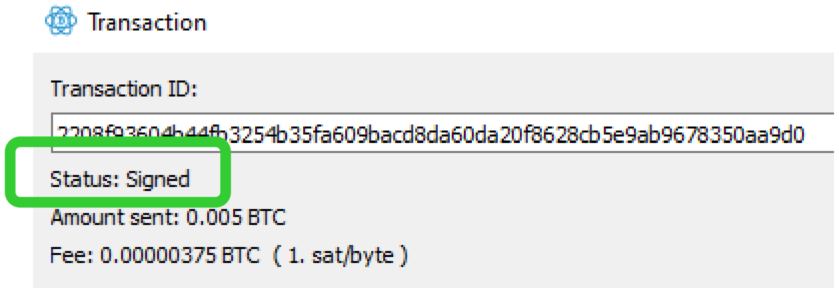
Size: 373 bytes
Replace by fee: True
LockTime: 1941368 (height)

Inputs (1)

```
f7a17e4ce458bc0db824c87c1f136845ff278bdeb9aad9796ada2a0ab57958b0:0     2N8Re7nApnyJjuZnHu5guMAQr3HmLNJx4G9     0.01869375
```

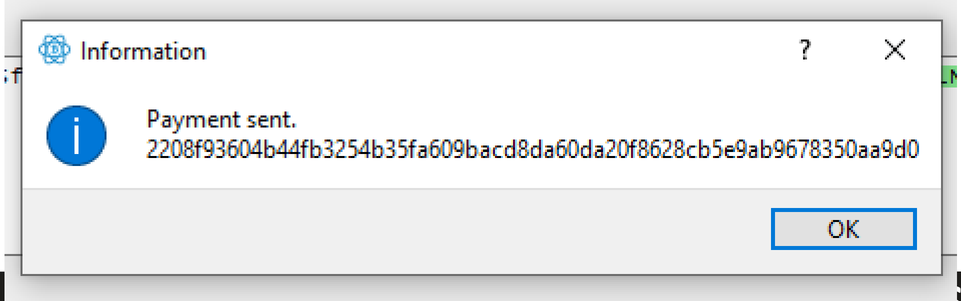
Outputs (2)

```
n3sQFihnho5YMvJJ3C8puFMQ1NreQystoa      0.005
2My4CFNSdzkJqv4riHFLtSS6UwGN4pGh4M6            0.01369
```



Transaction ID:
2208f93604b44fb3254b35fa609bacd8da60da20f8628cb5e9ab9678350aa9d0

Status: Signed
Amount sent: 0.005 BTC
Fee: 0.00000375 BTC (1. sat/byte)



Payment sent.
2208f93604b44fb3254b35fa609bacd8da60da20f8628cb5e9ab9678350aa9d0

Questions

- Analyze your transactions via blockchain explorer
  - E.g., https://blockstream.info/testnet/
  - TX (from normal to multisig wallet)
    - Can you figure that transaction was from normal to multisig?
    - If yes/no – what is the advantage / disadvantage?
  - TX (from multisig to normal wallet)
    - Can you recognize that input was multisig? How and Why?
  - How much was possible to save in fees by using segwit instead of legacy address?
- 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 him to spend your coins)? 1-of-3 or 3-of-3?
- What are advantages and disadvantages of 2-of-3 vs. 3-of-5?

COINJOIN / PAYJOIN TRANSACTIONS

symmetry.physio

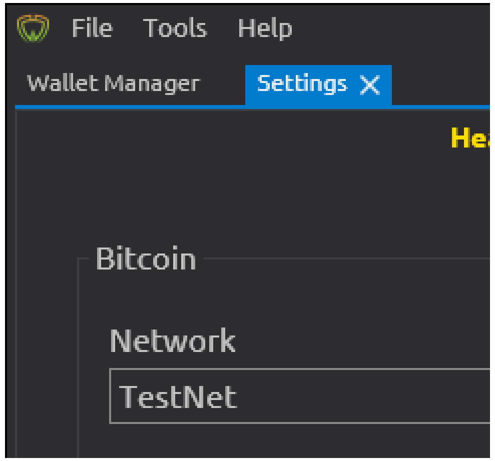
Analyze CoinJoin and PayJoin transactions

- Group of 3 students, share screen
- Example CoinJoin transactions
  - https://nioctib.tech/#/transaction/92a78def188053081187b847b267f0bfabf28368e9a7a642780ce46a78f551ba (example from https://en.bitcoin.it/wiki/CoinJoin)
  - https://blockstream.info/tx/c69aed505ca50473e2883130221915689c1474be3c66bcf7ac7dc0e26246afc8 (example from Wasabi wallet https://wasabiwallet.io/)
- Example PayJoin transaction
  - https://nioctib.tech/#/transaction/7104bae698587b3e75563b7ea7a9aada41d9c787788bc2bf26dd201fd7eca8a2
- Anything special in Lock and Unlock script?
- How can you find out if given TX is CoinJoin transaction?
- How can you find out if given TX is PayJoin transaction?

WASABI WALLET

Wasabi wallet (testnet)

- Solo task (1 students / breakout room)
- Install Wasabi wallet from https://wasabiwallet.io/
  - – For real use, verify PGP signature
- Start it, go to Settings and change Network to TestNet
- Restart application
- Generate new Wallet
  - – Backup seed, password is used to encrypt seed (if none, what it means?)
- Wasabi forces you to set coin label (Why?)
- Send some sats to Wasabi wallet from your normal testnet wallet



Bitcoin

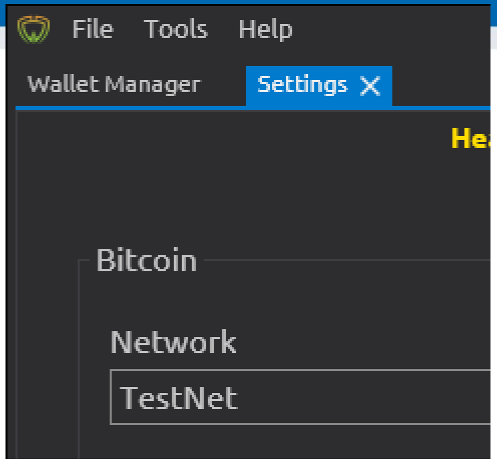
Network

TestNet

COINJOIN WITH WASABI WALLET

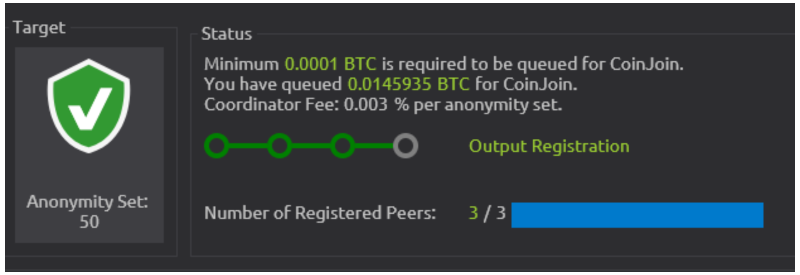
Wasabi wallet – participating in CoinJoin

- Visit CoinJoin option
  - – Change Target to Anonymity Set: 2 (so mixing finish quickly)
    - For real use, keep it 50!
  - – Enqueue Selected Coins into next round of CoinJoin
- Waits until registered and confirmed
- Keep your computer running
  - – The protocol is interactive, requires several rounds
- What have you got at the end?
- Investigate txid on chain explorer
  - – Use Tor, otherwise you will leak IP to TX mapping



Bitcoin

Network: TestNet

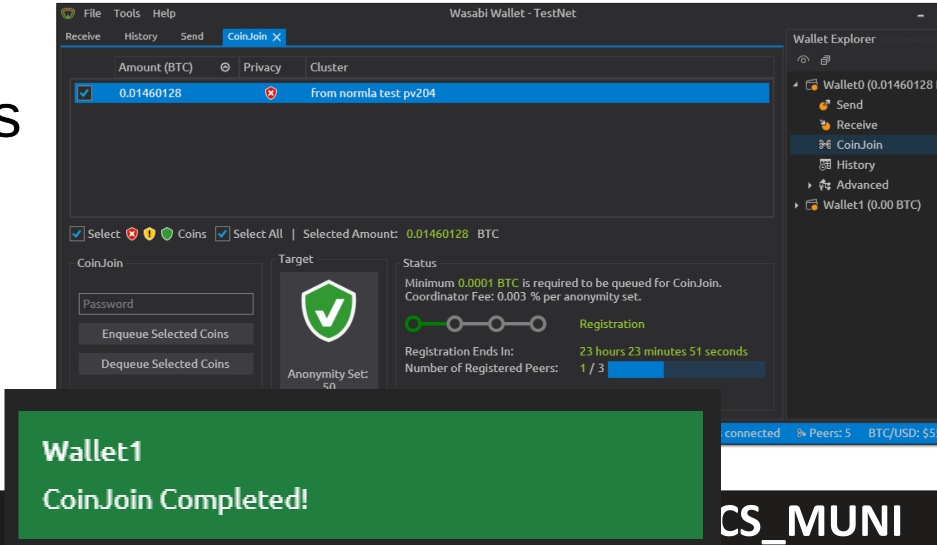


Anonymity Set: 50

Minimum 0.0001 BTC is required to be queued for CoinJoin.
You have queued 0.0145935 BTC for CoinJoin.
Coordinator Fee: 0.003 % per anonymity set.

Output Registration

Number of Registered Peers: 3 / 3



Wasabi Wallet - TestNet

	Amount (BTC)	Privacy	Cluster
☑	0.01460128	☒	from normla test pv204

Wallet0 (0.01460128

Wallet1 (0.00 BTC)

☑ Select ☒ ! ✓ Coins ☑ Select All | Selected Amount: 0.01460128 BTC

CoinJoin

Target: Anonymity Set: 50

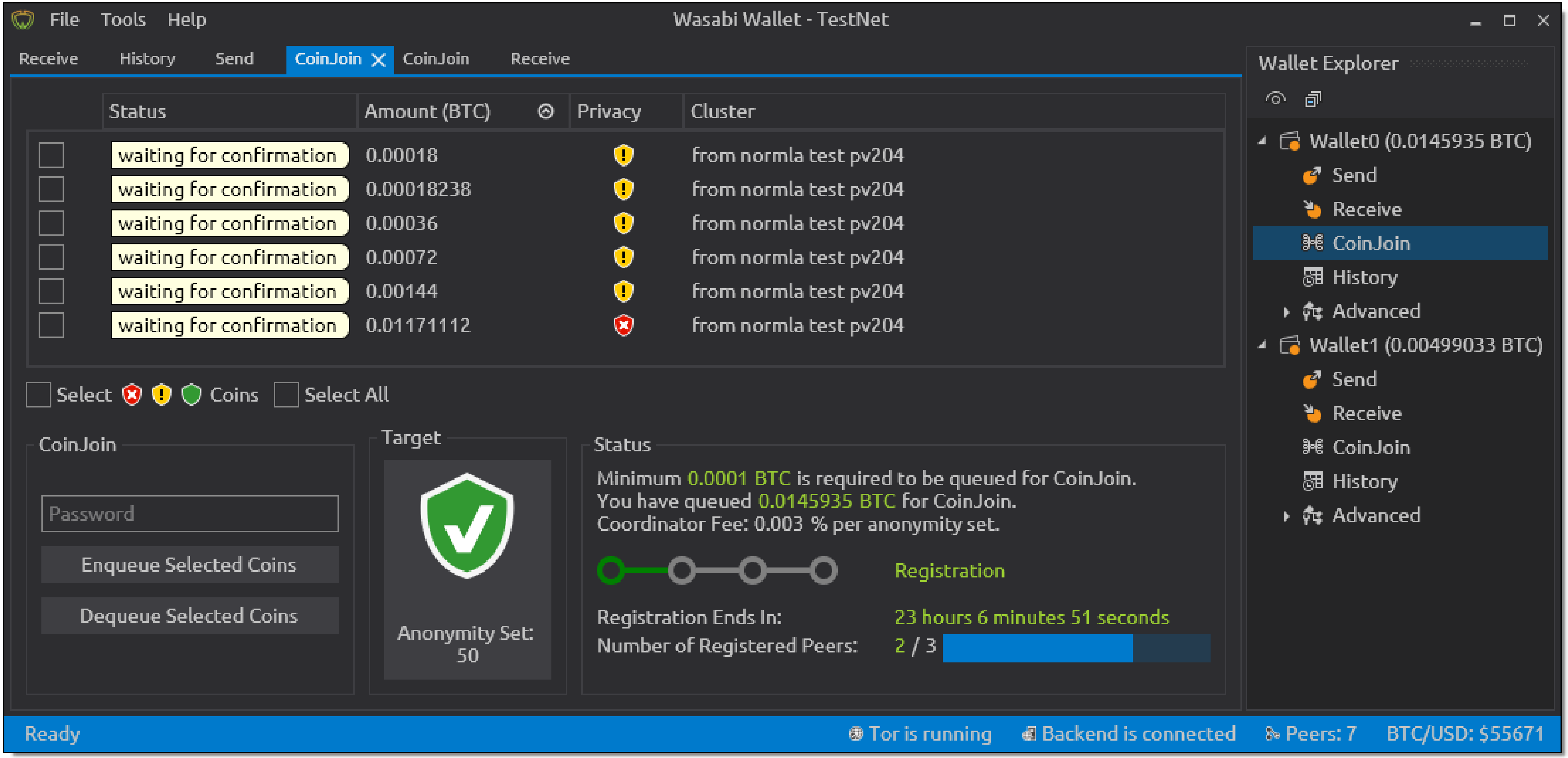
Status: Minimum 0.0001 BTC is required to be queued for CoinJoin.
Coordinator Fee: 0.003 % per anonymity set.

Registration

Registration Ends In: 23 hours 23 minutes 51 seconds
Number of Registered Peers: 1 / 3

connected Peers: 5 BTC/USD: $5

Wallet1
CoinJoin Completed!



	Status	Amount (BTC)	Privacy	Cluster
□	waiting for confirmation	0.00018	!	from normla test pv204
□	waiting for confirmation	0.00018238	!	from normla test pv204
□	waiting for confirmation	0.00036	!	from normla test pv204
□	waiting for confirmation	0.00072	!	from normla test pv204
□	waiting for confirmation	0.00144	!	from normla test pv204
□	waiting for confirmation	0.01171112	✕	from normla test pv204

Anonymity Set: 50

Status

Minimum 0.0001 BTC is required to be queued for CoinJoin.
You have queued 0.0145935 BTC for CoinJoin.
Coordinator Fee: 0.003 % per anonymity set.

Registration

Registration Ends In: 23 hours 6 minutes 51 seconds
Number of Registered Peers: 2 / 3

Ready | Tor is running | Backend is connected | Peers: 7 | BTC/USD: $55671

ASSIGNMENT

Assignment 4.1: Bitcoin network CLI

- Describe steps to create transaction with three outputs to three different addresses
  - List sequence of commands, add corresponding CLI screenshots
  - List raw resulting transaction
- Answer the following questions
  - Why bitcoins from regtest cannot be used on mainnet?
  - How is address on regtest different from mainnet?
  - When is mempool changing during your steps?

Assignment 4.2: Bitcoin transaction graph analysis

- Some bitcoins were sent mainnet on-chain by person X to other people (receivers)
  - The first transaction made will be called “original”, and was followed by several subsequent within 30 minutes interval (send->person + change address -> next person + change address …)
  - “original” Txid = f236bf1c11eea0f1d1d757ce31bd8dae8a400d5e3ef1a103b38e37081937ff2f
- Reconstruct and visualize graph of txs before and after “original”
- Answer the following questions
  - What are transaction IDs (txid) and output indexes (vout) for inputs of “original” transaction?
  - How much bitcoins person X owned before sending it to first other person (original tx)?
    - P.S. If you at some point deduce that X own more than 30 bitcoins, you are wrong ☺
  - From where “original” tx comes from (txid, additional analysis and discussion)?
  - What were receivers doing with the received sats?
  - How much fee was paid to create “original” UTXO?
  - What type of address was used? Was Segwit used?
  - What type of lock script was used? Was multisig used?

Assignment 4: Bitcoin

- Produce short text/pdf description of solution
  - – Provide steps for bitcoin regtest operations
  - – Provide visualization of transactions graph
  - – Provide answers to questions asked
- Submit before 14.4.2021 23:59 into IS HW vault (2 weeks)
  - – Soft deadline: -1.5 points for every started 24 hours