PV204 Security technologies

Cryptocurrencies II. - Bitcoin multisig, CoinJoin, PayJoin

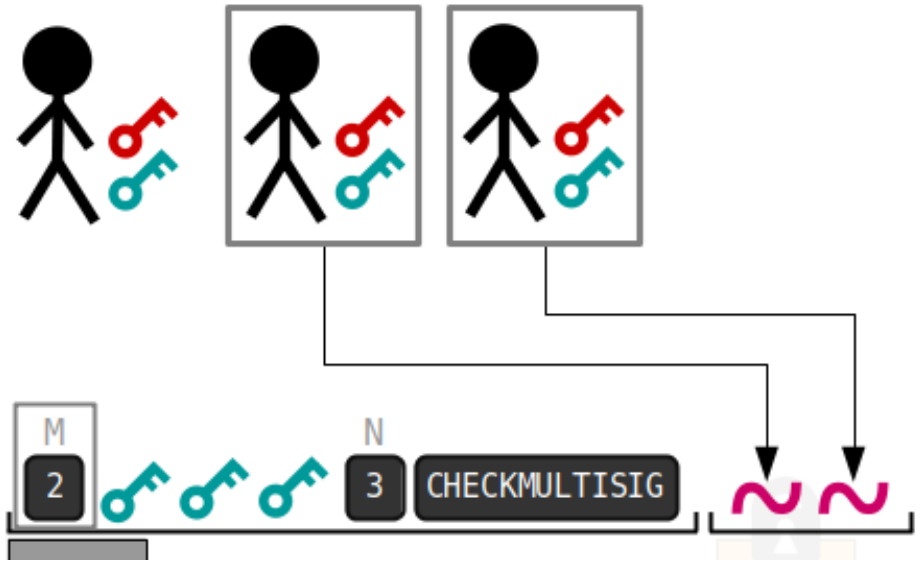
Petr Švenda *svenda@fi.muni.cz* *@rngsec*
Centre for Research on Cryptography and Security, Masaryk University

CROCS
Centre for Research on Cryptography and Security

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

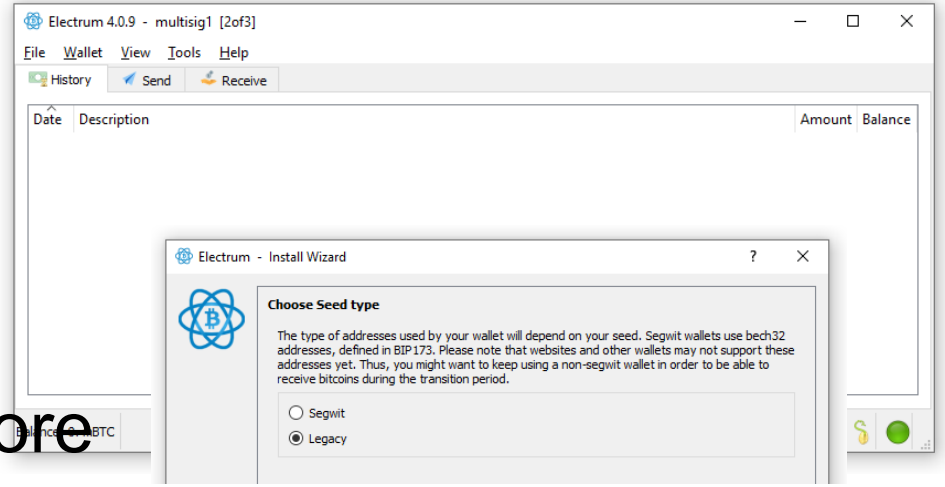


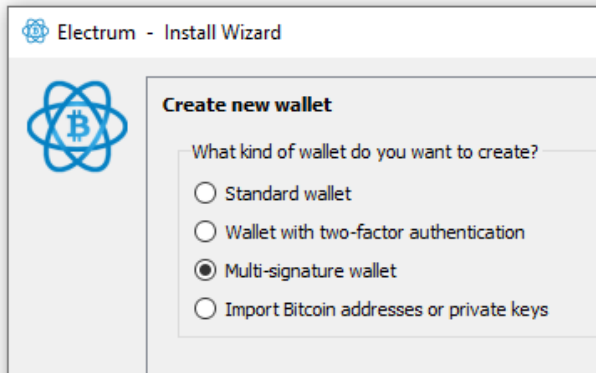
Task: using multisignature wallet (3ppl/room)

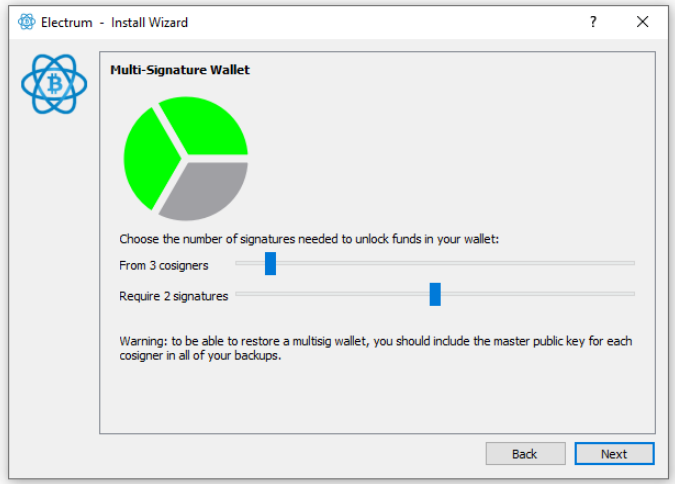
1. Create new 2-out-of-3 multisignature wallet in Electrum
   - All three people in the group are participants (separate machines)
2. Send some coins from last week to multisig wallet
   - Generate new receiving address
   - Wait till included in block
- Analyze TX (from normal to multisig) via chain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

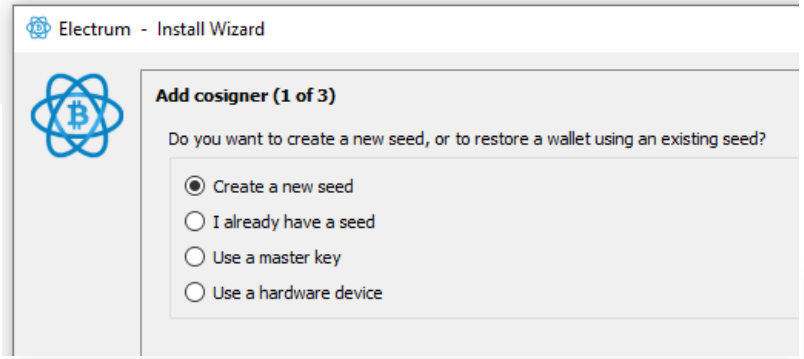
Creating multisig wallet (--testnet)

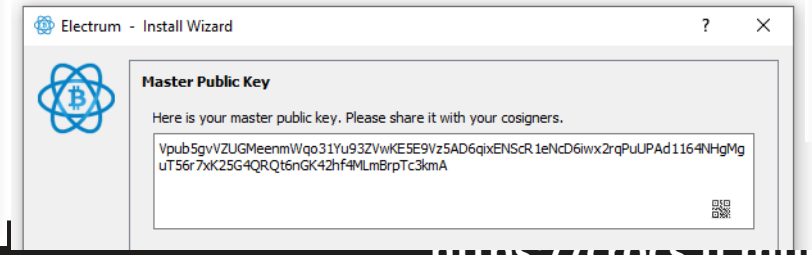
- If you already have wallet: File → New/Restore
  - All three people performs the same process, pick Legacy type (not segwit)
- Save seed and masterpub key for yourself (cosigner 1)
- Get masterpub key from others, Add cosigner (2 of 3), (3 of 3)
- Finish creation of multisig wallet

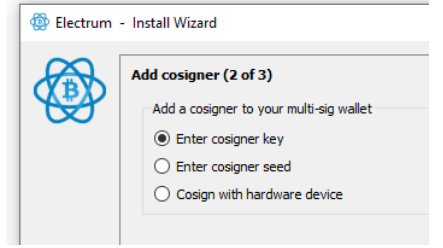


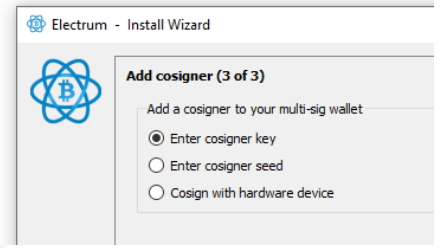






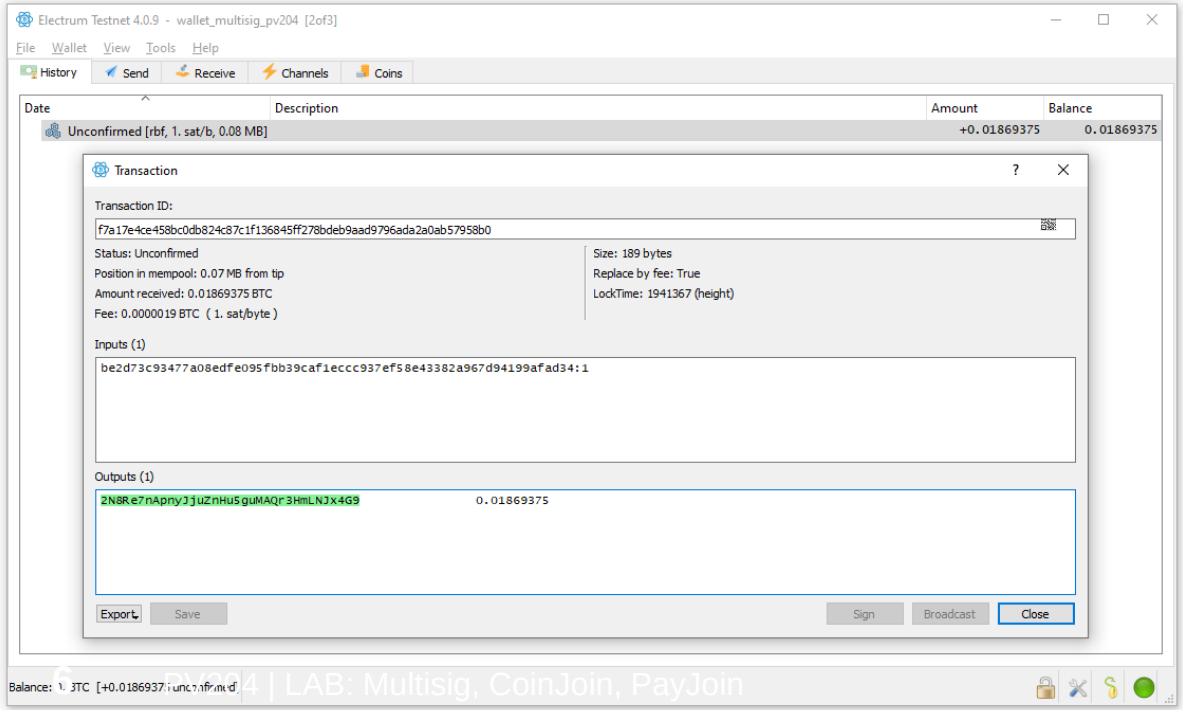


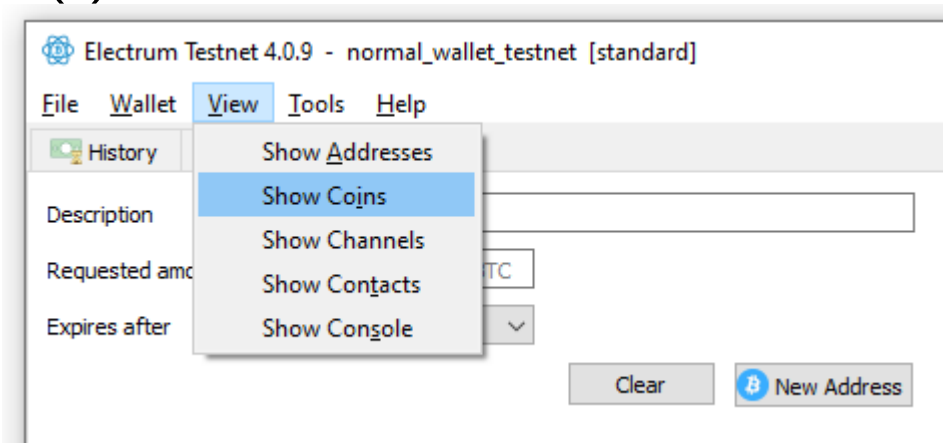




Send from normal wallet to multisig one

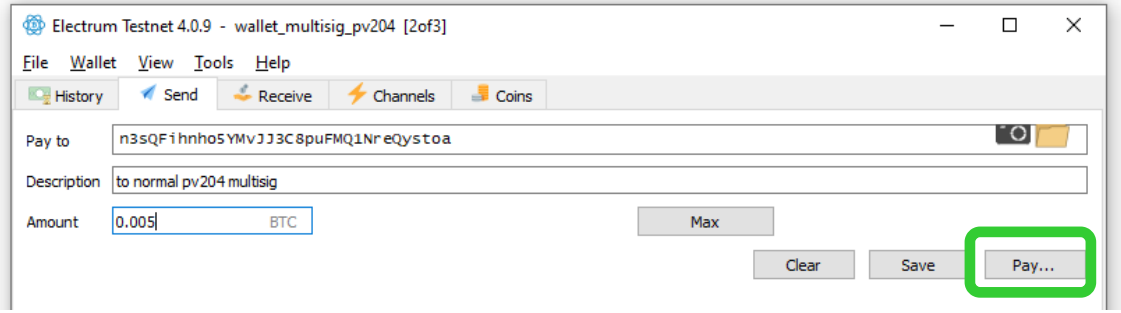
- Generate receive address on multisig, send to it from normal one
- Optional: try using coin control
  - View → Show coins, RClick on target coin → Spend
  - Max button in Send will only take marked coin(s)

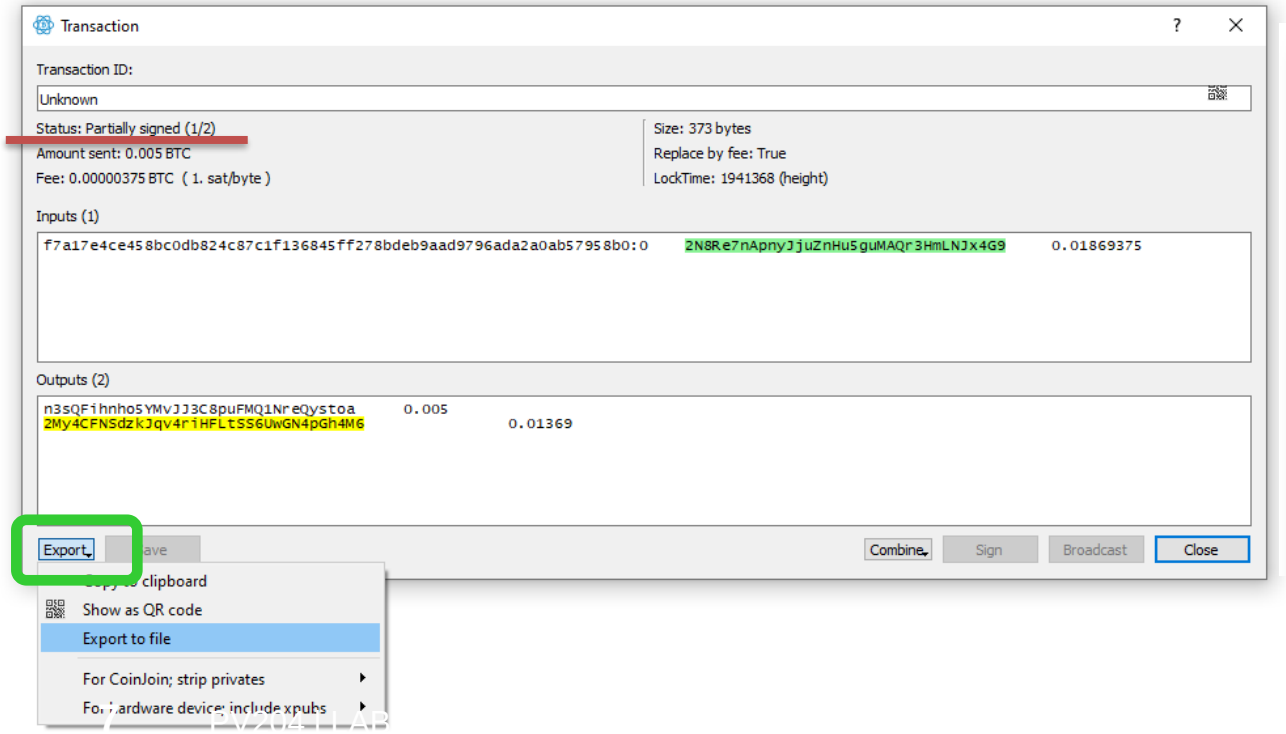


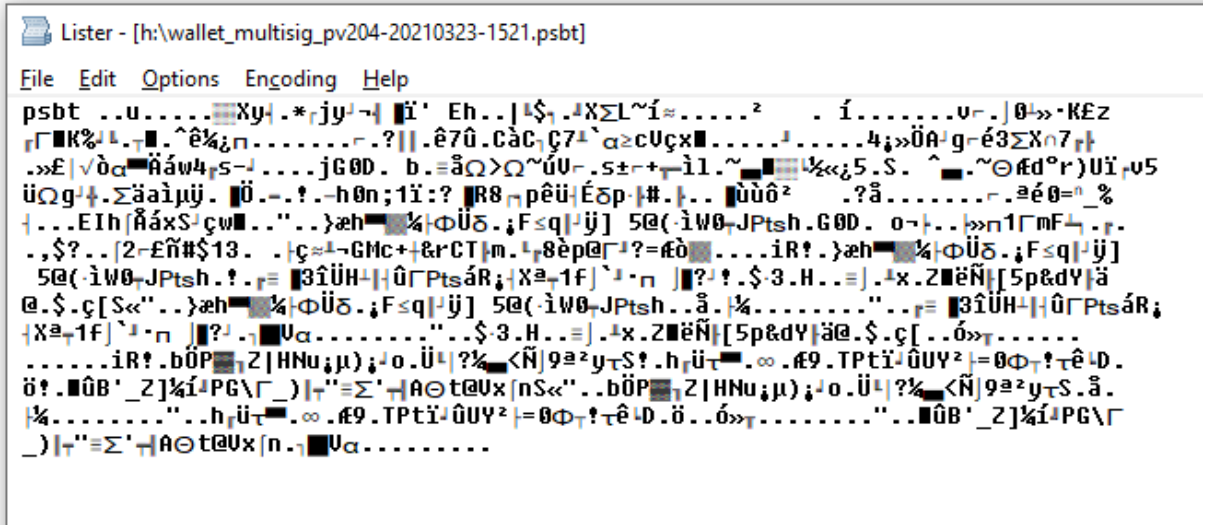


Send from multisig wallet to normal one – first signer

- 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

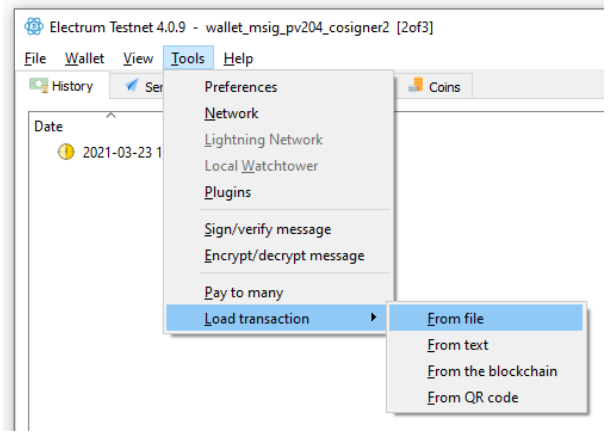


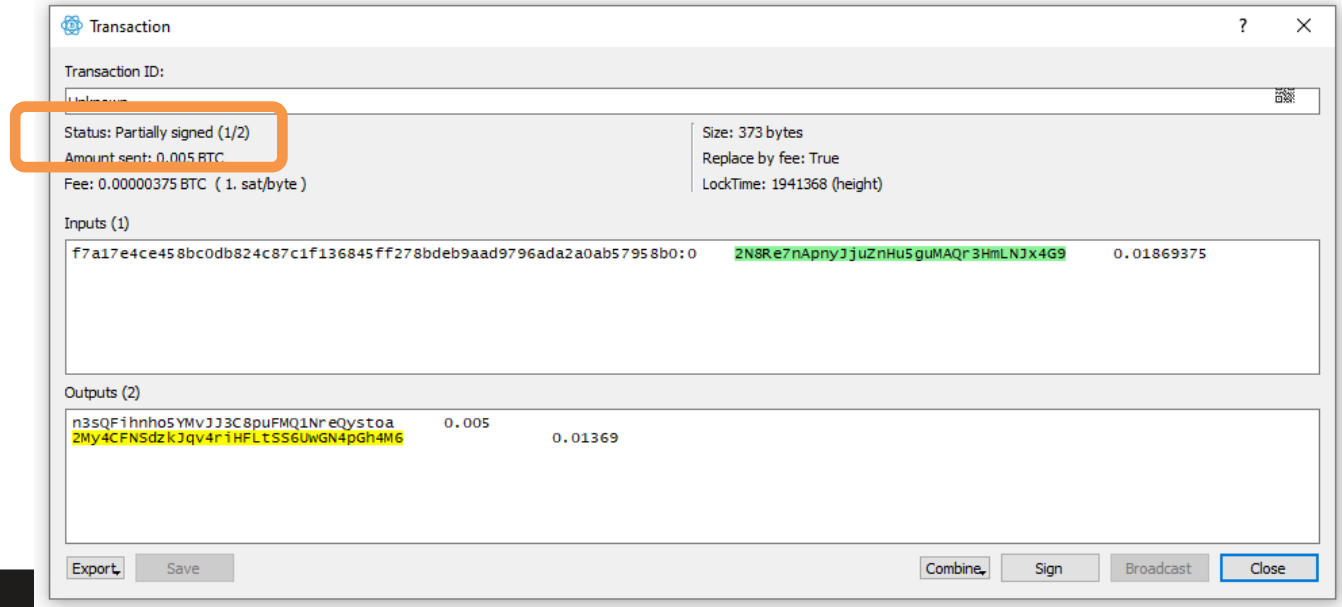


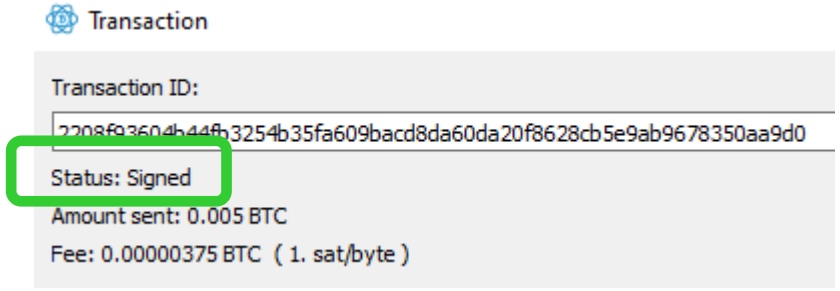


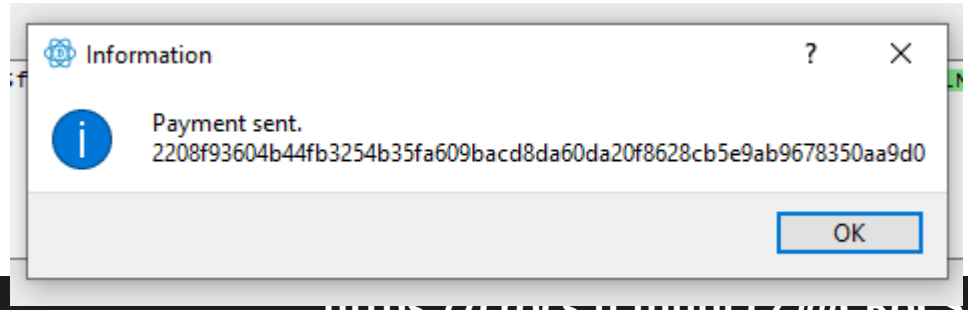
Send from multisig wallet to normal one – second signer

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









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?

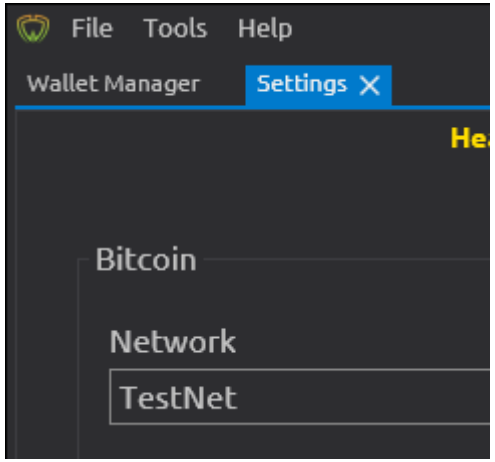
COINJOIN / PAYJOIN TRANSACTIONS

Analyze CoinJoin and PayJoin transactions ()

- Group of 3 students
- 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

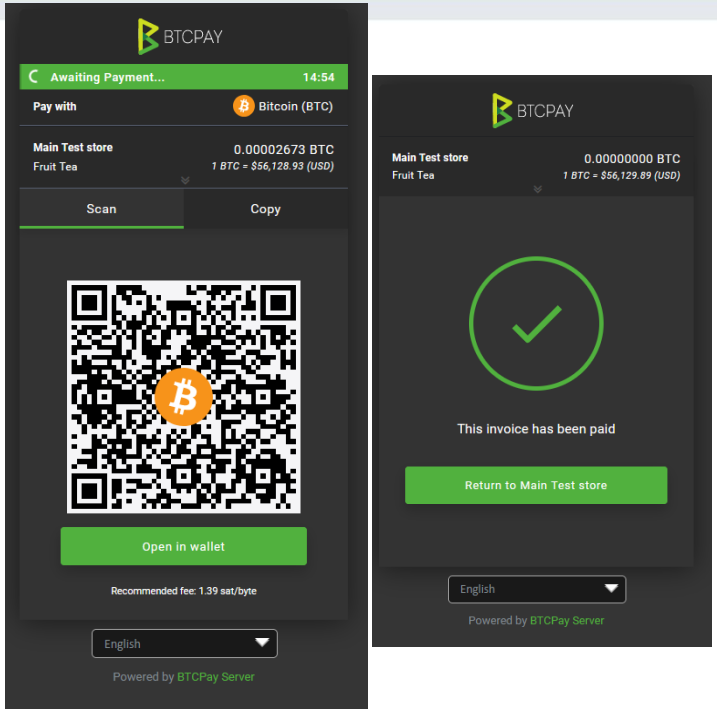
Wasabi wallet (testnet)



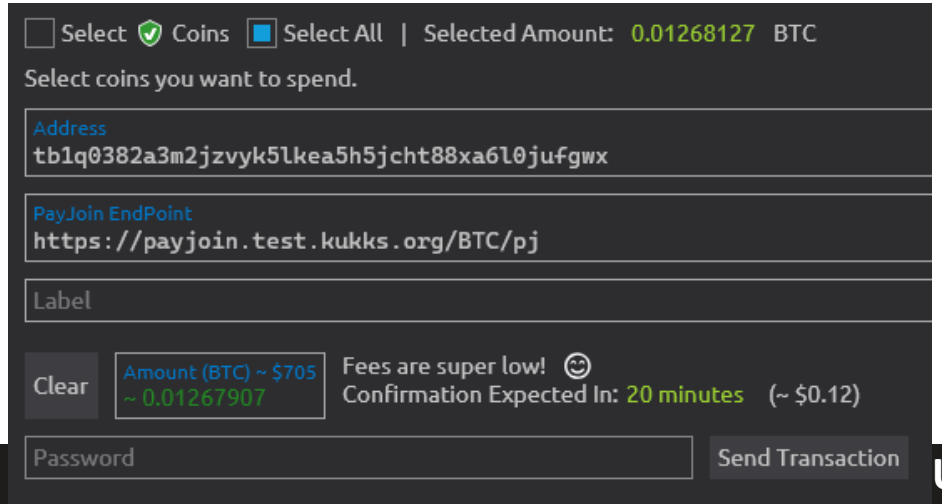
- Solo task (1 students / breakout room)
- Install Wasabi wallet from https://wasabiwallet.io/
- Start it, go to Settings and change Network to TestNet
- Restart application
- Generate new Wallet
  - Backup seed, password is used to encrypt seed (if none, what it means?)
- Wasabi forces you to set coin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

PAYJOIN WITH WASABI WALLET

Wasabi wallet – participating in PayJoin



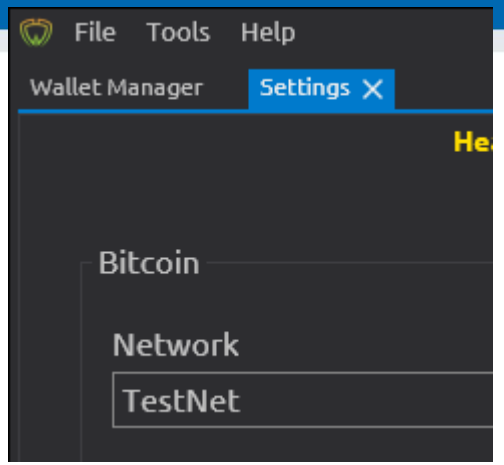
- Sending PayJoin step-by-step
  - https://docs.wasabiwallet.io/using-wasabi/PayJoin.html
- Go to https://payjoin.test.kukks.org/
  - Select tea you prefer, click Pay
  - Rclick on Open in wallet, copy link
  - bitcoin:tb1qux90y6k9mvf4nunny48r5rzurs8acjpedtrtlk?amount=0.00002673&pj=https://payjoin.test.kukks.org/BTC/pj
  - Paste it to Send, select one “coin”, Send tx
- Investigate txid on chain explorer
  - Copy txid from History tab
  - Use Tor, otherwise leak IP to TX mapping

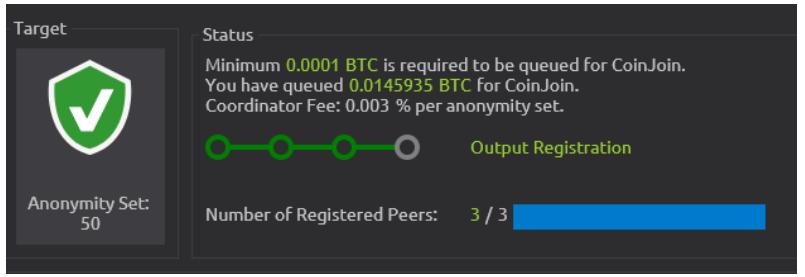


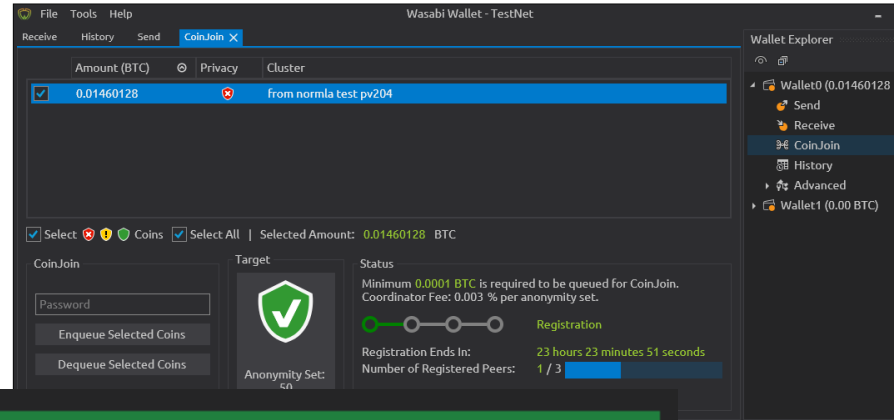
COINJOIN WITH WASABI WALLET

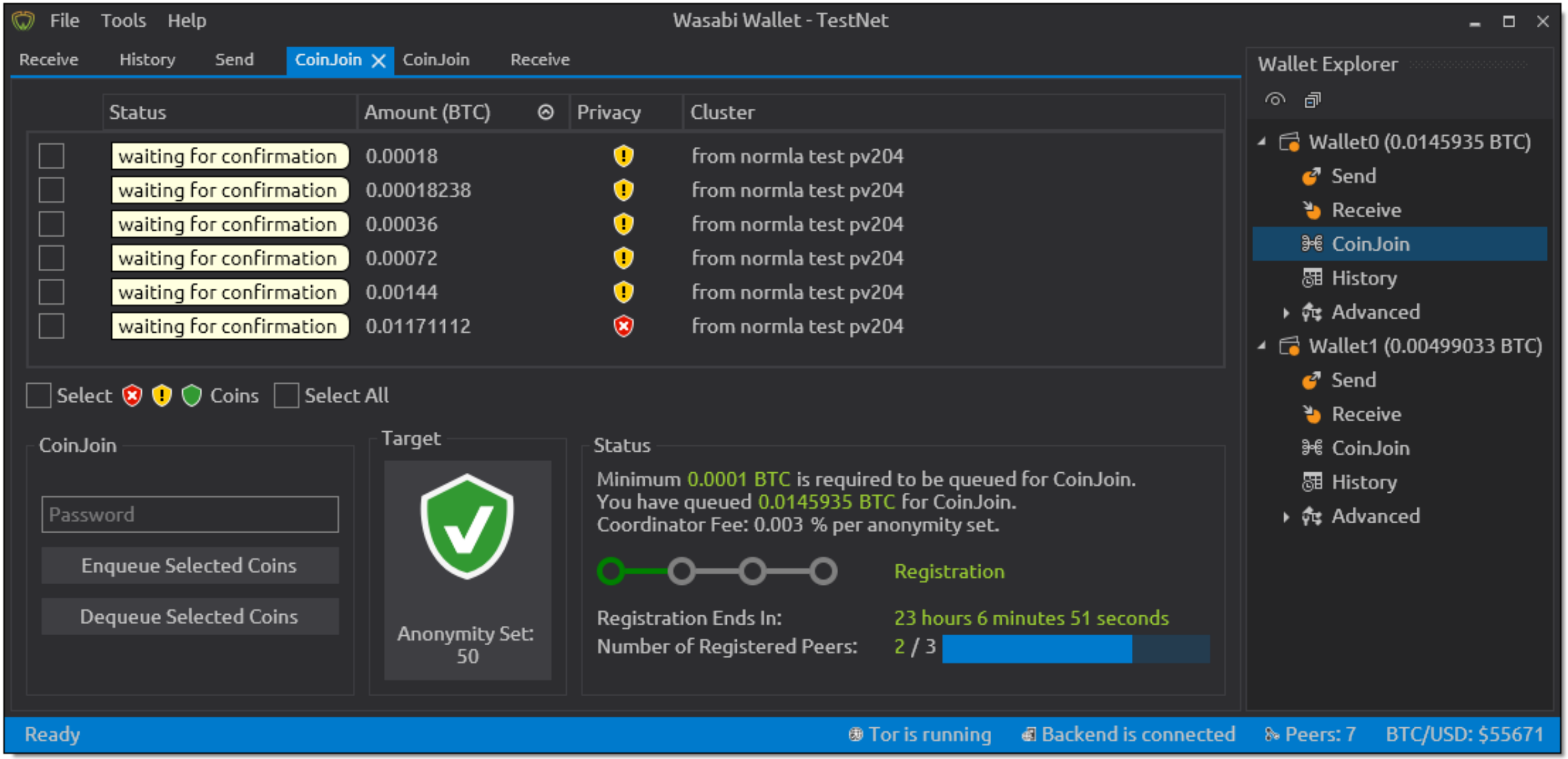
Wasabi wallet – participating in CoinJoin

- 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








File Tools Help
Wasabi Wallet - TestNet
Receive History Send CoinJoin CoinJoin Receive
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
Select Coins Select All
CoinJoin
Password
Enqueue Selected Coins
Dequeue Selected Coins
Target
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
Wallet Explorer
Wallet0 (0.0145935 BTC)
Send
Receive
CoinJoin
History
Advanced
Wallet1 (0.00499033 BTC)
Send
Receive
CoinJoin
History
Advanced
Ready
Tor is running
Backend is connected
Peers: 7
BTC/USD: $55671

NO NEW ASSIGNMENT THIS WEEK ☺
- ASSIGNMENT 2 TILL NEXT WEEK

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

Please rank topics covered this this seminar according to level of your interest

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