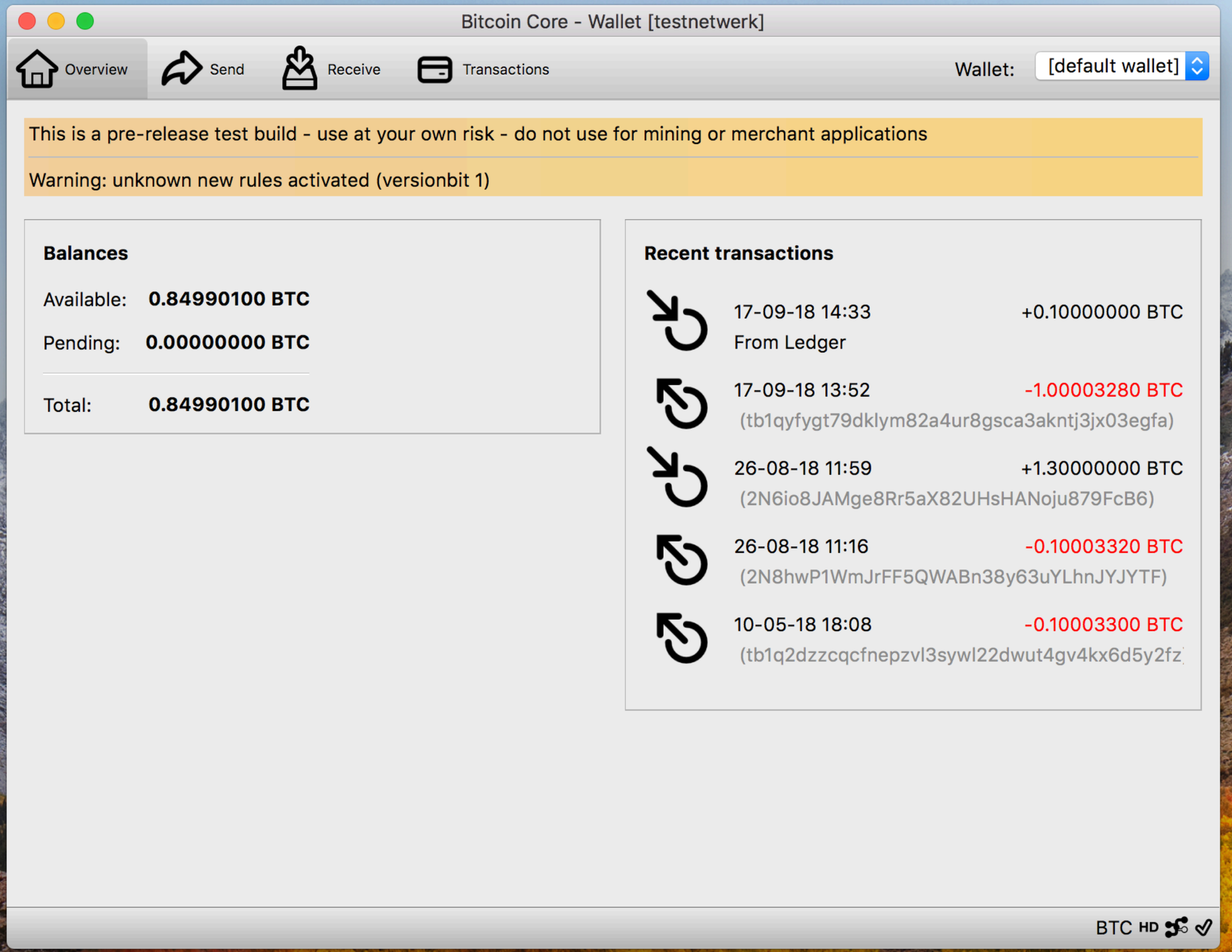
# Bitcoin Core wallet

1. Graphic User Interface (bitcoin-qt)
2. Commandline Interface (bitcoin-cli)


Bitcoin Core - Wallet [testnetwerk]
Overview
Send
Receive
Transactions
Wallet:
[default wallet]
This is a pre-release test build - use at your own risk - do not use for mining or merchant applications
Warning: unknown new rules activated (versionbit 1)
Balances
Available: 0.84990100 BTC
Pending: 0.00000000 BTC
Total: 0.84990100 BTC
Recent transactions
17-09-18 14:33 +0.10000000 BTC
From Ledger
17-09-18 13:52 -1.00003280 BTC
(tb1qyfygt79dklym82a4ur8gsca3akntj3jx03egfa)
26-08-18 11:59 +1.30000000 BTC
(2N6io8JAMge8Rr5aX82UHsHANoju879FcB6)
26-08-18 11:16 -0.10003320 BTC
(2N8hwP1WmJrFF5QWABn38y63uYLhnJYJYTF)
10-05-18 18:08 -0.10003300 BTC
(tb1q2dzzcqcfnepzvl3sywl22dwut4gv4kx6d5y2fz
BTC HD

3. bash

```
g4WFT:bitcoind bitcoin$ bitcoin-cli listtransactions | jq
[
  {
    "address": "2NDLwfkyEa8TdQpzzGxwPQhYC58v4sQXJPd",
    "category": "receive",
    "amount": 0.65,
    "label": "Faucet",
    "vout": 0,
    "confirmations": 116658,
    "blockhash": "000000000127f6c55faa6a5bb856afc1db9da7d5aa3a4ba3ac06339be2d27d9c",
    "blockindex": 7,
    "blocktime": 1525971620,
    "txid": "e9dd91a0c63aae7de112cfa056bf063c687085e52b818fa7f15a5fb63038afd2",
    "walletconflicts": [],
    "time": 1525970878,
    "timereceived": 1525970878,
    "bip125-replaceable": "no"
  },
  {
    "address": "tb1q2dzzcqcfnepzvl3sywl22dwut4gv4kx6d5y2fz",
    "category": "send",
    "amount": -0.1,
    "label": "",
    "vout": 1,
    "fee": -3.3e-05,
    "confirmations": 116657,
    "blockhash": "00000000000000fd90f0f9a455057206e522b8298c6b488c2fd9c3014111f39c",
    "blockindex": 58,
    "blocktime": 1525972516,
    "txid": "38a605a7bd309e2108ff3bdaabfcb51b3f0e326595a958f2741dd54a849923dd",
    "walletconflicts": [],
    "time": 1525972117,
    "timereceived": 1525972117,
    "bip125-replaceable": "no",
    "abandoned": false
  },
  {
    "address": "2N8hwP1WmJrFF5QWABn38y63uYLhnJYJYTF",
    "category": "send",
    "amount": -0.1,
    "label": "",
    "vout": 0,
    "fee": -3.32e-05,
    "confirmations": 4060,
    "blockhash": "0000000000000041e5949283868237c19ce9d19397524e5f7f58b47e60fc4c7a",
```

# Bitcoin Core wallet

» validates all blocks

» well reviewed code

» sits on your computer

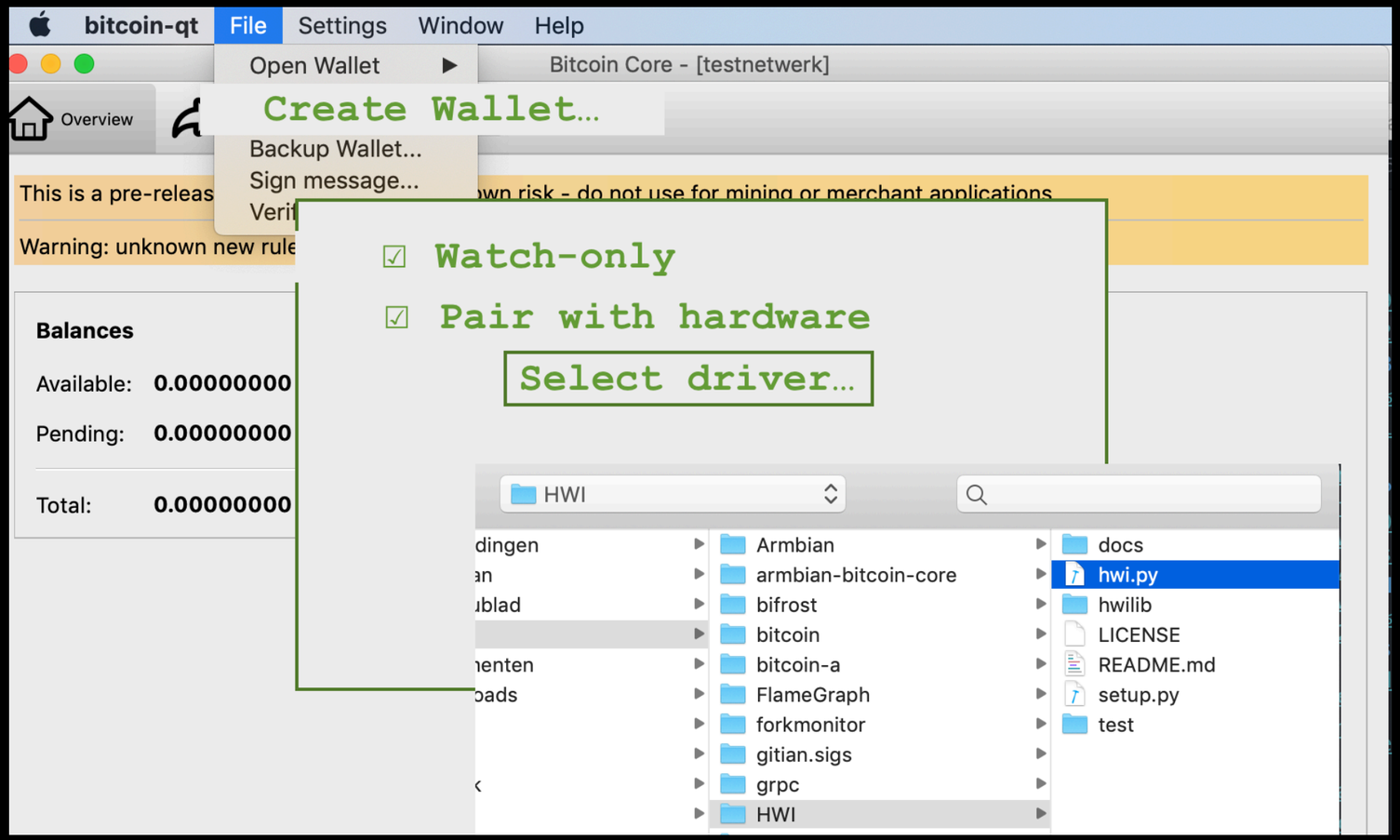
# Hardware Wallet

- not on your computer
- reveals addresses to 3rd party
- relies on external truth (e.g. SegWit2x)
- lots of (wallet) code

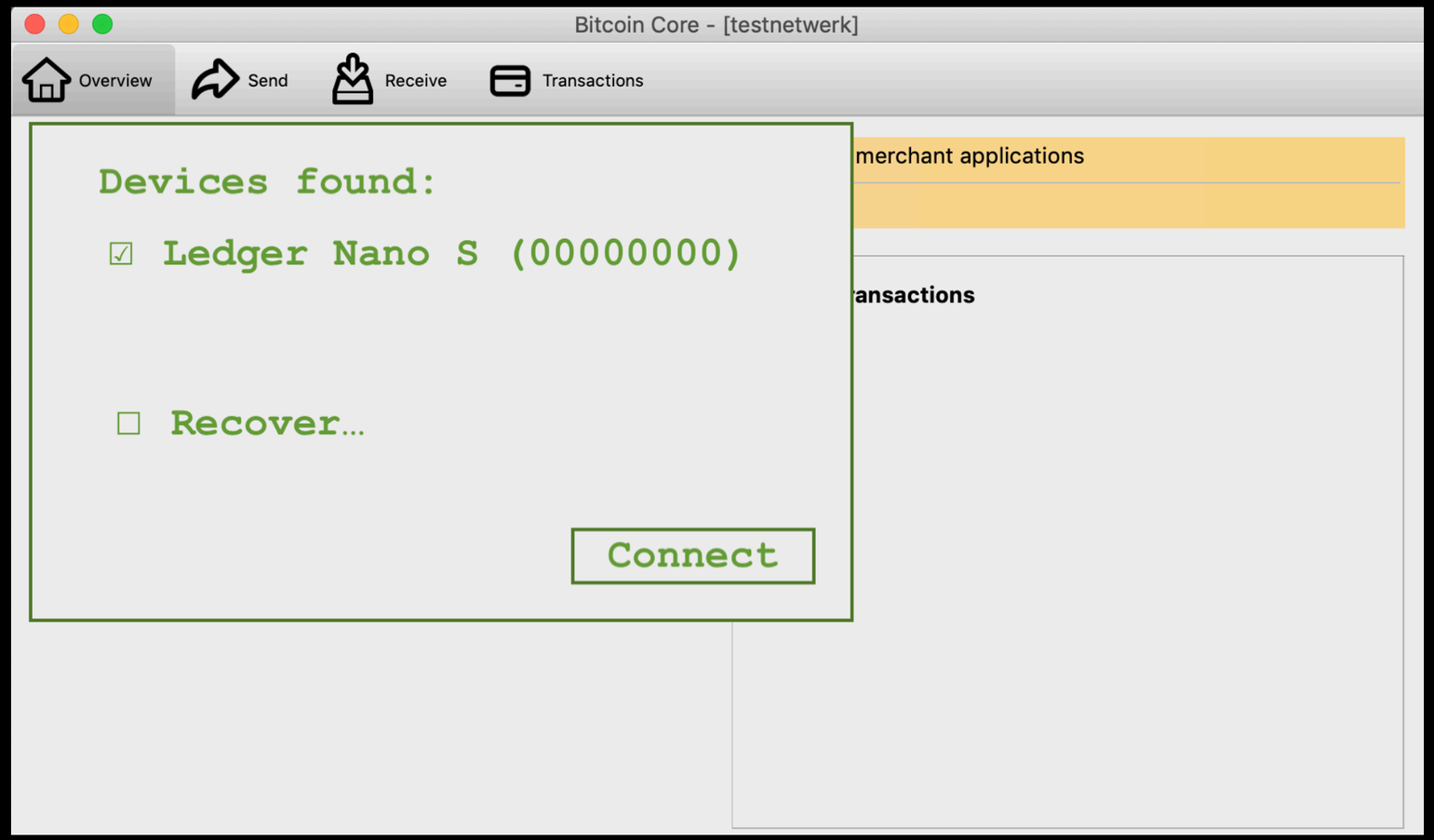
# Combined

- keys not on your computer
- great privacy
- no external truth
- only hardware specific code to review

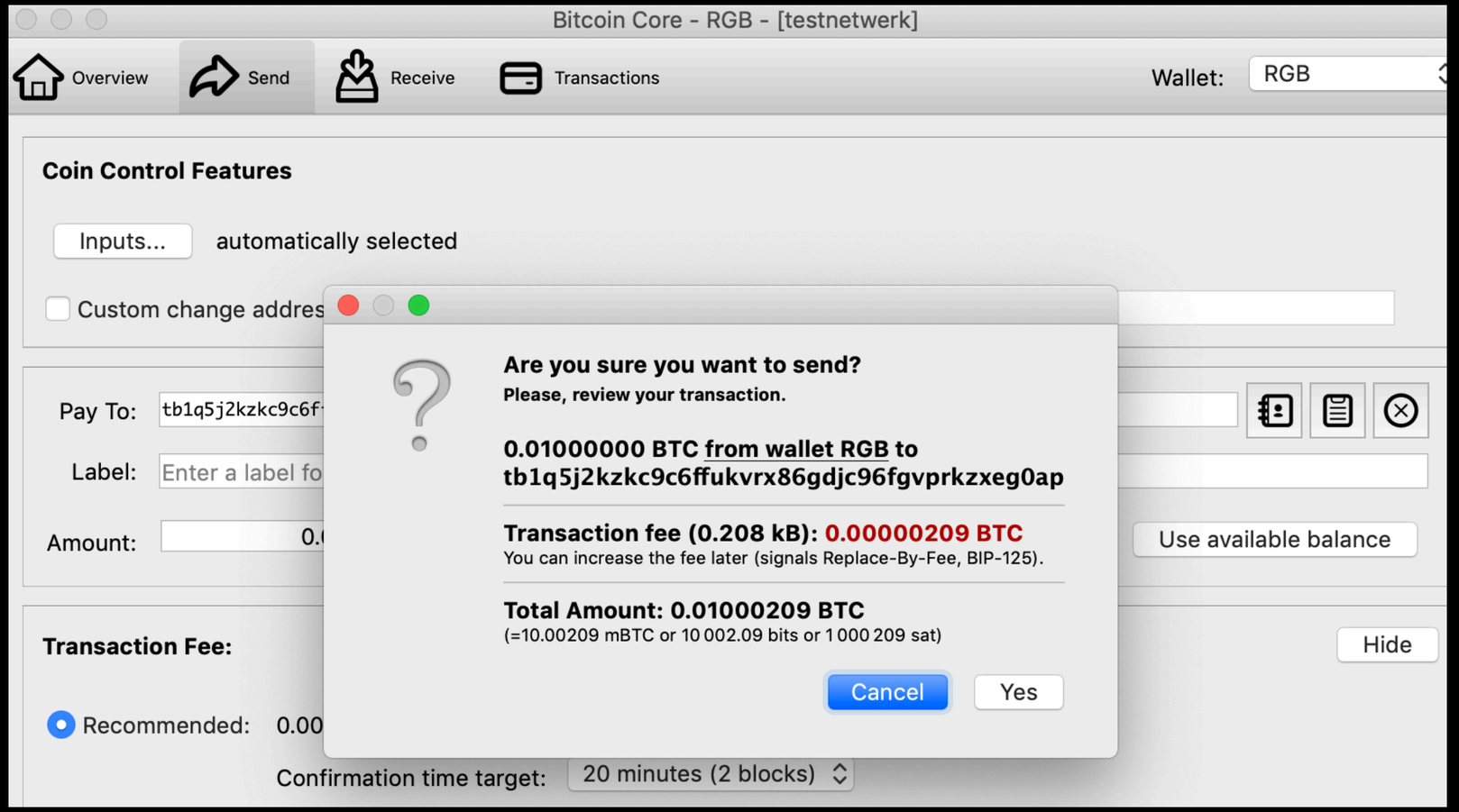
# Ideally


bitcoin-qt
File
Settings
Window
Help
Open Wallet
Bitcoin Core - [testnetwerk]
Overview
Create Wallet...
Backup Wallet...
Sign message...
Verif
This is a pre-releas
own risk - do not use for mining or merchant applications
Warning: unknown new rule
Balances
Available: 0.00000000
Pending: 0.00000000
Total: 0.00000000
☑ Watch-only
☑ Pair with hardware
Select driver...
HWI
dingen
an
ublad
menten
oads
Armbian
armbian-bitcoin-core
bifrost
bitcoin
bitcoin-a
FlameGraph
forkmonitor
gitian.sigs
grpc
HWI
docs
hwi.py
hwilib
LICENSE
README.md
setup.py
test

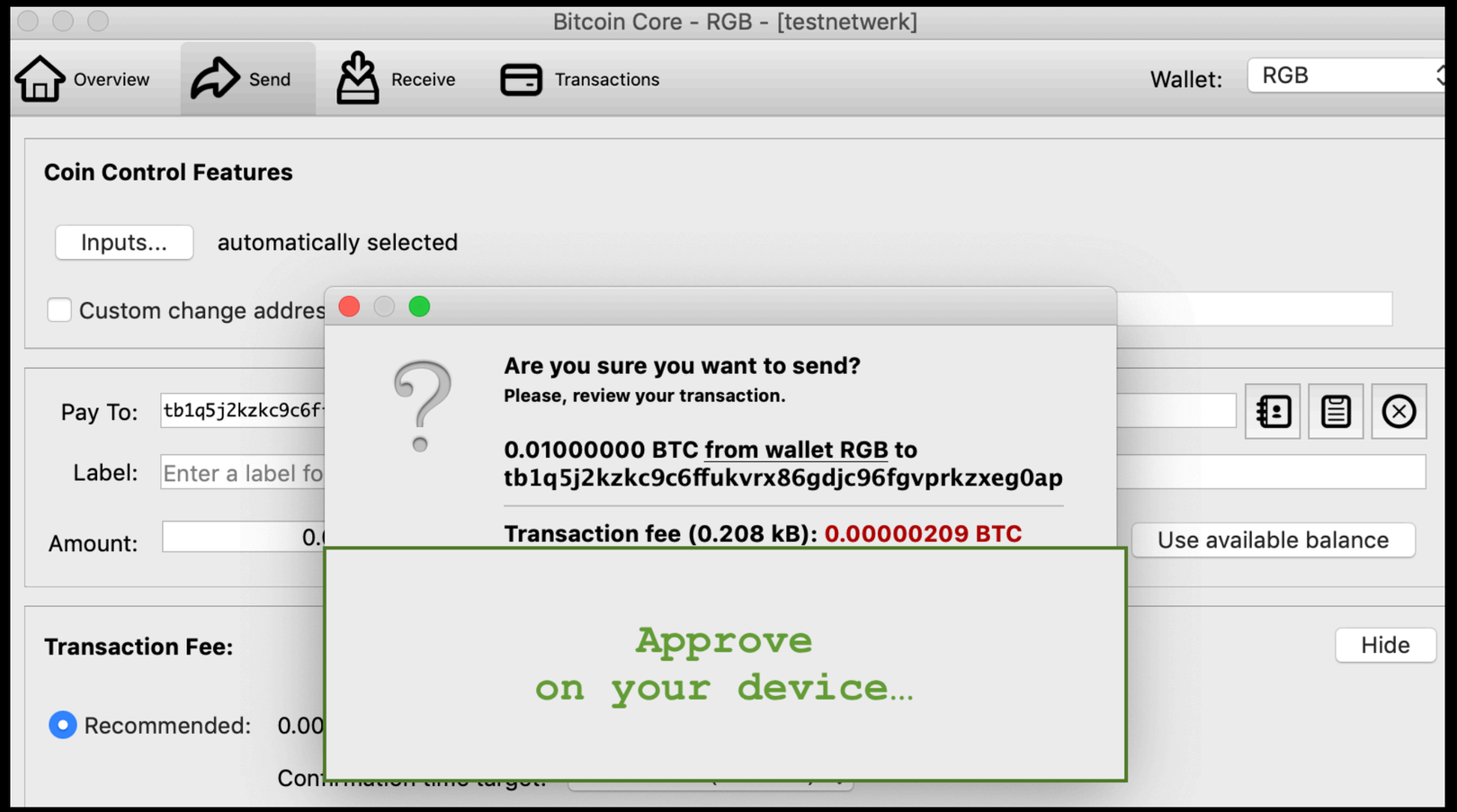
# Ideally


Bitcoin Core - [testnetwerk]
Overview
Send
Receive
Transactions
merchant applications
ansactions
Devices found:
☑ Ledger Nano S (00000000)
☐ Recover...
Connect

# Ideally


Bitcoin Core - RGB - [testnetwerk]
Overview
Send
Receive
Transactions
Wallet:
RGB
Coin Control Features
Inputs...
automatically selected
Custom change addres
Pay To:
tb1q5j2kzkc9c6f
Label:
Enter a label fo
Amount:
Use available balance
Transaction Fee:
Hide
Recommended:
0.00
Confirmation time target:
20 minutes (2 blocks)
Are you sure you want to send?
Please, review your transaction.
0.01000000 BTC from wallet RGB to
tb1q5j2kzkc9c6ffukvrx86gdjc96fgvprkzxeg0ap
Transaction fee (0.208 kB): 0.00000209 BTC
You can increase the fee later (signals Replace-By-Fee, BIP-125).
Total Amount: 0.01000209 BTC
(=10.00209 mBTC or 10 002.09 bits or 1 000 209 sat)
Cancel
Yes

# Ideally


Bitcoin Core - RGB - [testnetwerk]
Overview
Send
Receive
Transactions
Wallet:
RGB
Coin Control Features
Inputs...
automatically selected
Custom change addres
Pay To:
tb1q5j2kzkc9c6f
Label:
Enter a label fo
Amount:
Use available balance
Transaction Fee:
Hide
Recommended:
0.00
Are you sure you want to send?
Please, review your transaction.
0.01000000 BTC from wallet RGB to
tb1q5j2kzkc9c6ffukvrx86gdjc96fgvprkzxeg0ap
Transaction fee (0.208 kB): 0.00000209 BTC
Approve
on your device...

# In reality

1. Electrum Personal Server (works now! v0.16+)
2. Python scripts: HWI[6] (v0.18?)
3. HWI + Bitcoin Core RPC (v0.19?)
4. GUI (v0.20+)

[6] Hardware Wallet Integration: https://github.com/bitcoin-core/HWI

# Electrum Personal Server[5]

» install Bitcoin Core

» install Electrum

» install Electrum Personal Server

» small config change… profit!

[5] https://github.com/chris-belcher/electrum-personal-server

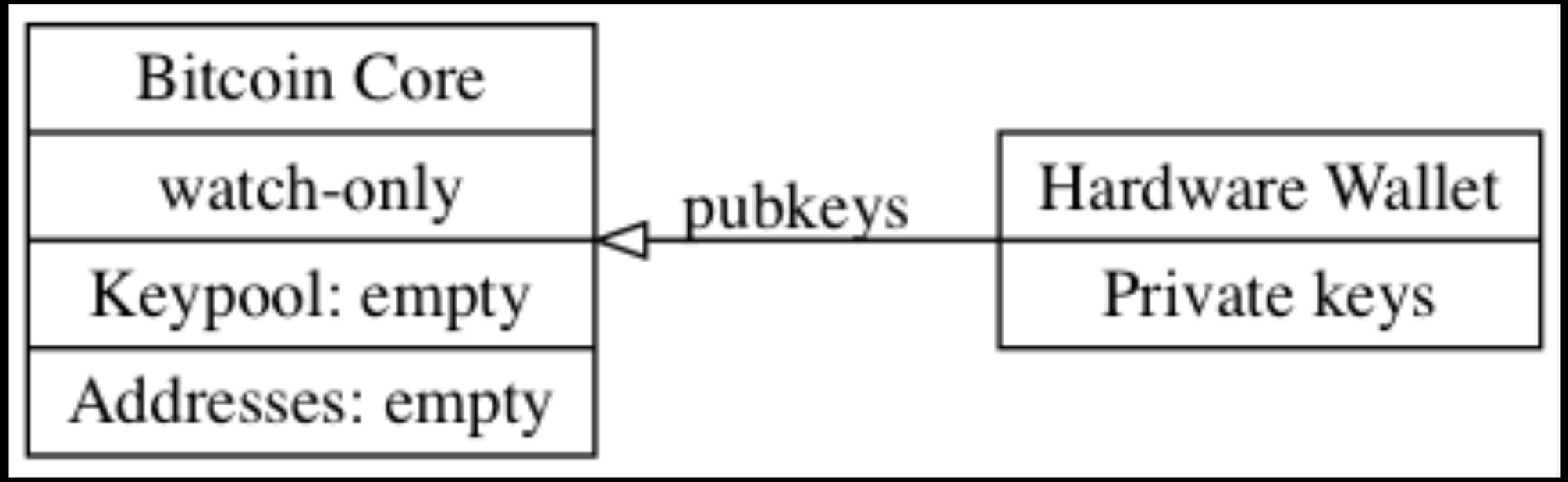
# Problems

- how to encode transaction data? PSBT
- how to communicate between device and Core wallet?
  - (unix) pipes
  - JSON RPC
- minimize amount of stuff to install
- not too radical changes to Bitcoin Core

# Core + HWW Setup

» Start with empty watch-only wallet

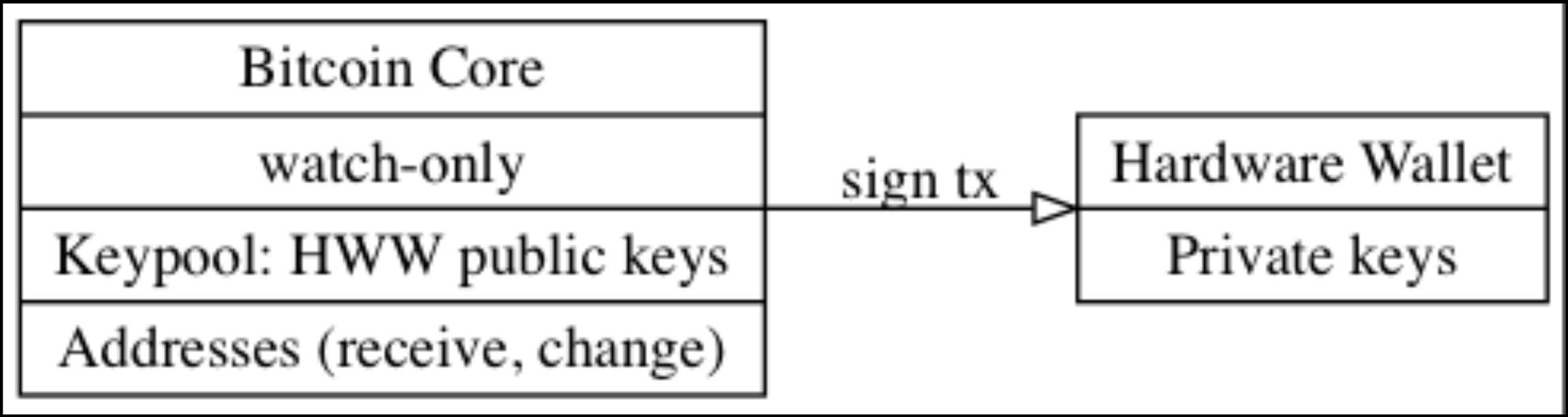
» Import public keys from device



# Core + HWW Usage

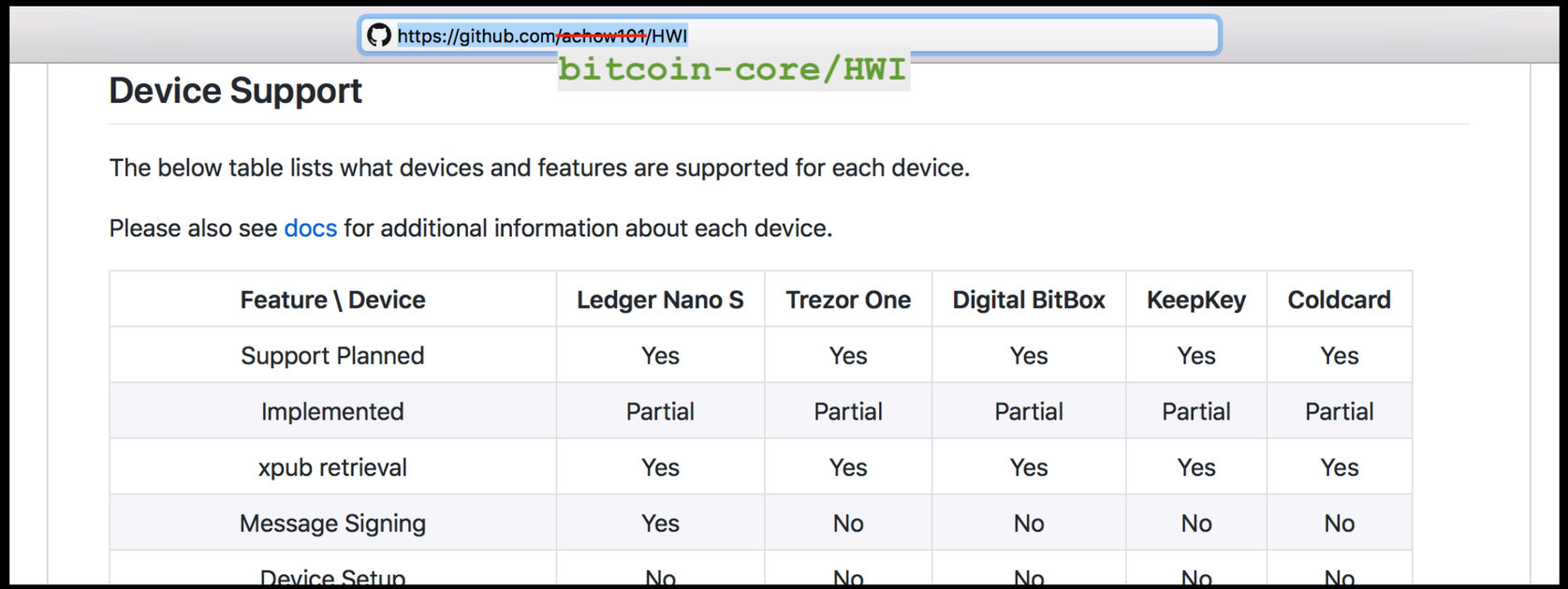
» Generate unsigned transaction in Core

» Sign on device



# HWI

» Bitcoin Hardware Wallet Interaction scripts[0] by Andrew Chow




[0] https://github.com/bitcoin-core/HWI

# List devices

```
g4WFT:HWI bitcoin$ ./hwi.py enumerate | jq
[
  {
    "type": "ledger",
    "path": "IOService:/AppleACPIPlatformExpert/PCI0@0/AppleACPIPCI/XHC1@14/XHC1@14000000
/HS02@14200000/Nano S@14200000/Nano S@0/IOUSBHostHIDDevice@14200000,0",
    "serial_number": "0001",
    "fingerprint": "d9d676d4"
  },
```

» Fingerprint (of master xpub): used as identifier

```
g4WFT:~ bitcoin$ bitcoin-cli createwallet "ledger" true
{
  "name": "ledger",
  "warning": ""
}
g4WFT:~ bitcoin$ bitcoin-cli -rpcwallet=ledger getwalletinfo
{
  "walletname": "ledger",
  "walletversion": 169900,
  "balance": 0,
  "unconfirmed_balance": 0,
  "immature_balance": 0,
  "txcount": 0,
  "keypoololdest": 1537360584,
  "keypoolsize": 0,
  "paytxfee": 0,
  "private_keys_enabled": false
}
```

# Create watch-only wallet

Usefull stuff added in v0.17.0:

» dynamic wallet create / load / unload

» watch-only wallets

# Get keys from device

» BIP32, e.g. native segwit: m/84'/1'/'0/{0,1}/*'

```
g4WFT:HWI bitcoin$ ./hwi.py --testnet --fingerprint c8df832a getxpub "m/84'/1'/0'"
{
  "xpub": "tpubDDUZtWPP8YWdJfeBjSFe4ugo67eGD4m5BV6Hfyb57ZNXihydbiy6yHwdii5NPaM29DRo
}
```

» "wpkh([c8df832a/84'/1'/0']tpubDDUZ...zka/0/*)"

# Output Descriptors[7]

>> `wpkh([c8df832a/84'/1'/0']tpubDDUZ...zka/0/*)`

>> or `pkh(../44'/...)` for legacy addresses

>> or `multi(2,`
`[0000001/84'/1'/0']tpubDDUZ...zka/0/\*,`
`[0000002/84'/1'/0']tpubEEXZ...fab/0/\*)`

[7] https://github.com/bitcoin/bitcoin/blob/master/doc/descriptors.md

# Import keys into wallet

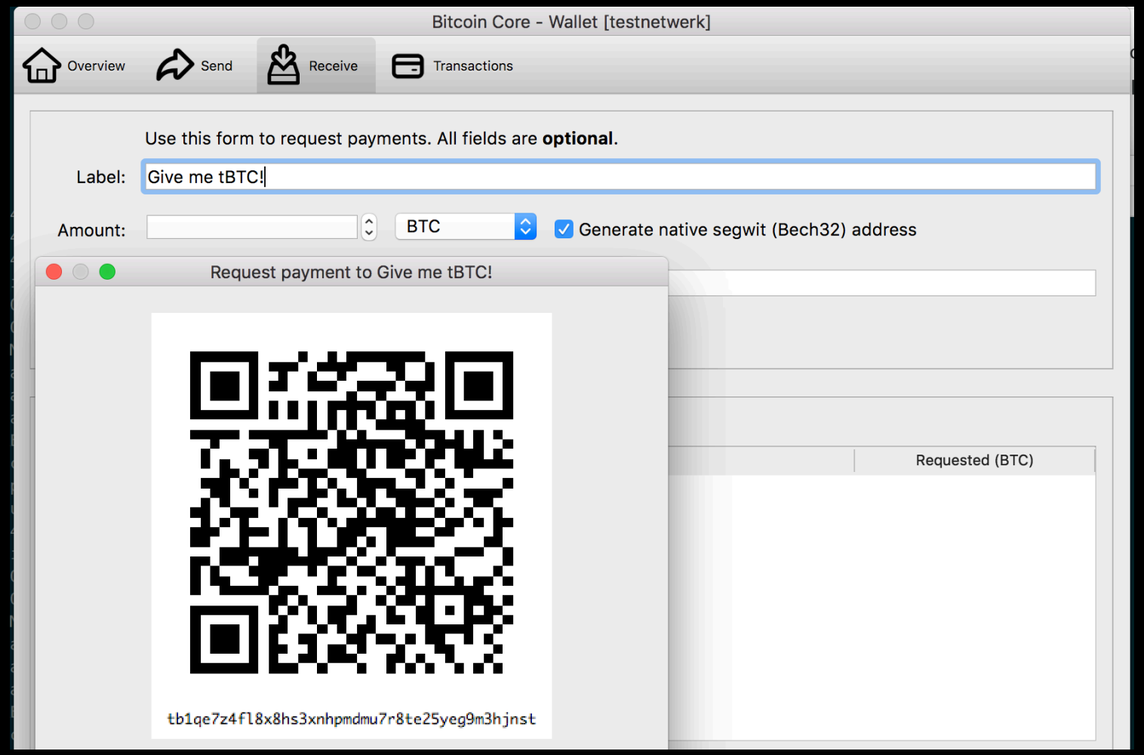
- `importmulti` RPC (v0.18?)
  - descriptor support (MeshCollider[2])
  - add imported keys to keypool (achow101[8])

[2] https://github.com/bitcoin/bitcoin/pull/14491

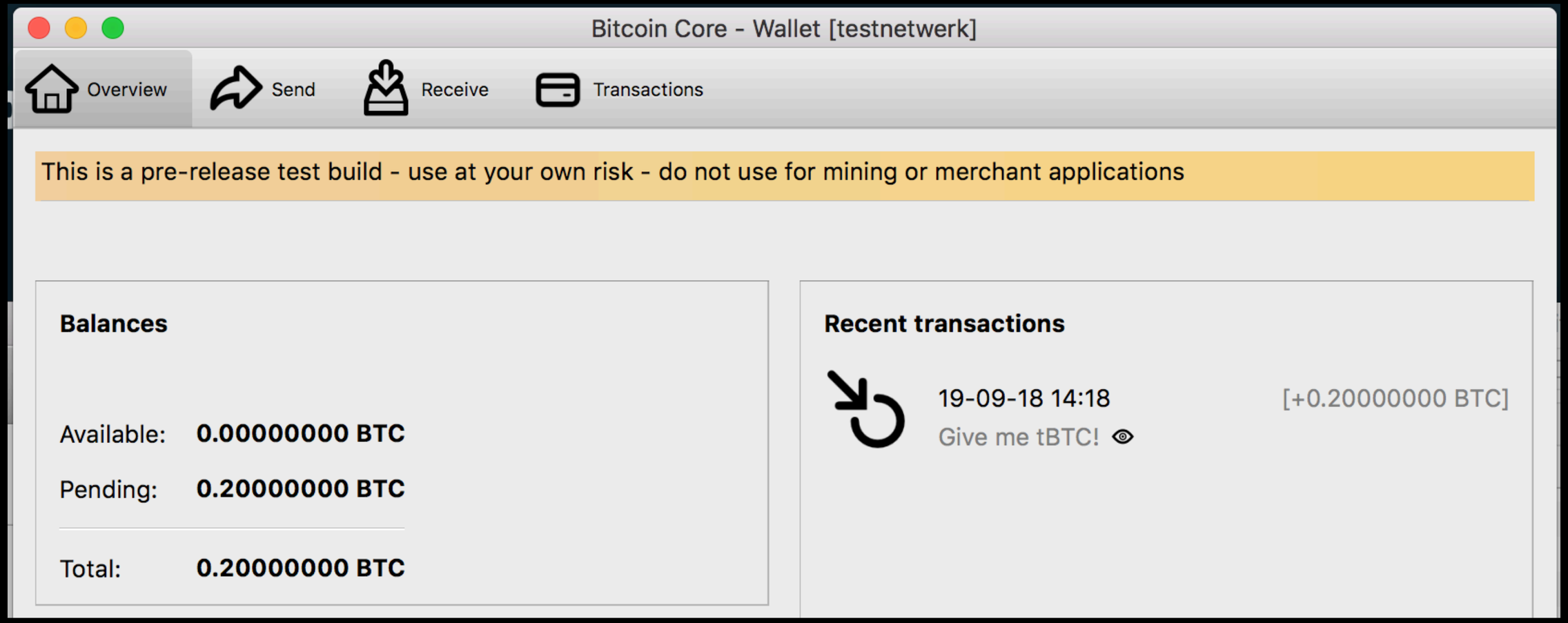
[8] https://github.com/bitcoin/bitcoin/pull/14075

# Generate receive address

» no hardware device needed!



# Wait for confirmation



# Prepare transaction
## The hard way

```
g4WFT:HWI bitcoin$ bitcoin-cli -rpcwallet=ledger walletcreatefundedpsbt '[]' '[{"tb1qap9up5dm9ksxcppu3mvnev7ass6k6nljps3le6":0.1}]'
0 '{"includeWatching":true}' true | jq
{
  "psbt": "cHNidP8BAJoCAAAAAgurCz3eBSqicMZiLL4j36ROZdkfbbEY/DX+BW0LV38pAQAAAAD+////C6sLPd4FKqJwxmIsviPfpE5l2R9tsRj8Nf4FbQtXfykAAAAA
P7///8CgJaYAAAAAAAWABToS8DRuy2gbAQ8jtk8s92ENW1P8iGVmAAAAAAAFgAU8zA9MNe5DssPlBkwG1WvsebjoUkAAAAAAAEBH4CWmAAAAAAAFgAUz4VU/OY94RNO4dt3z
wzryqhMoLsiBgPYSY/CRyUJYTDh+FY+QHEJQ54sndJiZAVIM/psslY/SRjZ1nbUVAAAgAEAAIAAAACAAAAAAAAAAAAAAAQEf85WYAAAAAAAWABTCsrCq24f82P3KdgXrZOgt0
CNPvCIGAo81Lov+Zkyk3vl1Yfo14LgGiWS9KnqMJlHOIY8B/muHGNnWdtRUAACAAQAAgAAAAIABAAAAAAAAAAAAAIgIDPU8aMJAgXoQPyn6E7LrLc/eNbdLQLztsIgGJZ5k7A
VAY2dZ21FQAAIABAACAAAAAgAEAAAABAAAAAA==",
  "fee": 2.1e-06,
  "changepos": 1
}
```

» note: `{includeWatching: true}`

» note: `true` at the end adds HD paths

# PSBT

» Partially Signed Bitcoin Transaction

» Added to v0.17.0

# Sign transaction


```
g4WFT:HWI bitcoin$ ./hwi.py --testnet --fingerprint d9d676d4 signtx cHNidP8BAHECAAAAAdXJ58haj4oqocs6kza+noYvjjuc0CmMh4uHyNzwYJ90AQAAAAD+////AvOVmAAAAAAAFgAUwrKwqtuH/Nj9ynYF62ToLdAjT7yAlpgAAAAAABYAFM+FVPzmPeETTuHbd88M68qoTKC7AAAAAAABAR8ALTEBAAAAABYAFM+FVPzmPeETTuHbd88M68qoTKC7IgID2EmPwkclCWEw4fhWPkBxCUOeLJ3SYmQFSDP6bLJWP0kY2dZ21FQAAIABAACAAAAAgAAAAAAAAAAAACICAo81Lov+zyk3l1Yb14LgGiv9KnMJlhDIY8/muHGhWdtRUAACAQAAgAAAAAAAAAAAAAAAAAAAAAAiAgPYSY/CRyUJYTDh+FY+QHEJQ54sndJiZAVIM/psslY/SRjZ1nbUVAAAgAEAAIAAAACAAAAAAAAAAAAA
{"psbt": "cHNidP8BAHECAAAAAdXJ58haj4oqocs6kza+noYvjjuc0CmMh4uHyNzwYJ90AQAAAAD+////AvOVmAAAAAAAFgAUwrKwqtuH/Nj9ynYF62ToLdAjT7yAlpgAAAAAABYAFM+FVPzmPeETTuHbd88M68qoTKC7AAAAAAABAR8ALTEBAAAAABYAFM+FVPzmPeETTuHbd88M68qoTKC7IgID2EmPwkclCWEw4fhWPkBxCUOeLJ3SYmQFSDP6bLJWP0lHMEQCIEq0nebj70u7x37n67hm4/HDbqTeJaKC2utU1Dh6nwJaAiAe/nP2GMNJihXA6xNP0qm+Rlly6gunnfyitzIjD5sRHgEiBgPYSY/CRyUJYTDh+FY+QHEJQ54sndJiZAVIM/psslY/SRjZ1nbUVAAAgAEAAIAAAACAAAAAAAAAAAAAAAAAIgICjzUui/5mTKTe+XVh+jXguAaJZL0qeowmUc4hjwH+a4cY2dZ21FQAAIABAACAAAAAgAEAAAAAAAAACICA9hJj8JHJQlhMOH4Vj5AcQlDniyd0mJkBUgz+myyVj9JGNnWdtRUAACAQAAgAAAIAAAAAAAAAAAA="}
```


"inputs": [
{
"witness_utxo": {
"amount": 0.2,
"scriptPubKey": {
"asm": "0 cf8554fce63de1134ee1db77cf0cebcaa84ca0bb",
"hex": "0014cf8554fce63de1134ee1db77cf0cebcaa84ca0bb",
"type": "witness_v0_keyhash",
"address": "tb1qe7z4f
}
},
"bip32_derivs": [
{
"pubkey": "03d8498fc24725096130e1f8563e407109439e2c9dd26264054833fa6cb2563f49",
"master_fingerprint": "d9d676d4",
"path": "m/84'/1'/0'/0/0"
}
]
}
],
Before

```
  "inputs": [
    {
      "witness_utxo": {
        "amount": 0.2,
        "scriptPubKey": {
          "asm": "0 cf8554fce63de1134ee1db77cf0cebcaa84ca0bb",
          "hex": "0014cf8554fce63de1134ee1db77cf0cebcaa84ca0bb",
          "type": "witness_v0_keyhash",
          "address": "tb1qe7z4fl8x8hs3xnhpmdmu7r8te25yeg9m3hjnst"
        }
      },
      "partial_signatures": {
        "03d8498fc24725096130e1f8563e407109439e2c9dd26264054833fa6cb2563f49": "304402204ab49
de6e3ef4bbbc77ee7ebb866e3f1c36ea4de25a282daeb54d4387a9f025a02201efe73f618c3498a15c0eb134fd2a
9be465972ea0ba79dfca2b732230f9b111e01"
      },
      "bip32_derivs": [
        {
          "pubkey": "03d8498fc24725096130e1f8563e407109439e2c9dd26264054833fa6cb2563f49",
          "master_fingerprint": "d9d676d4",
          "path": "m/84'/1'/0'/0/0"
        }
      ]
    }
  ],
```


After

# Finalize and broadcast

```
g4WFT:HWI bitcoin$ bitcoin-cli -rpcwallet=ledger finalizepsbt "cHNidP8BAHECAAAAAdXJ58haj4oqo
cs6kza+noYvjjuc0CmMh4uHyNzwYJ90AQAAAAD+////AvOVmAAAAAAAFgAUwrKwqtuH/Nj9ynYF62ToLdAjT7yAlpgAA
AAAABYAFM+FVPzmPeETTuHbd88M68qoTKC7AAAAAAABAR8ALTEBAAAAABYAFM+FVPzmPeETTuHbd88M68qoTKC7IgID2
EmPwkclCWEw4fhWPkBxCUOeLJ3SYmQFSDP6bLJWP0lHMEQCIEq0nebj70u7x37n67hm4/HDbqTeJaKC2utU1Dh6nwJaA
iAe/nP2GMNJihXA6xNP0qm+Rlly6gunnfyitzIjD5sRHgEiBgPYSY/CRyUJYTDh+FY+QHEJQ54sndJiZAVIM/psslY/S
RjZ1nbUVAAAgAEAAIAAAACAAAAAAAAAAAAAIgICjzUui/5mTKTe+XVh+jXguAaJZL0qeowmUc4hjwH+a4cY2dZ21FQAA
IABAACAAAAAgAEAAAAAAAAAACICA9hJj8JHJQlhMOH4Vj5AcQlDniyd0mJkBUgz+myyVj9JGNnWdtRUAACAAQAAgAAAA
IAAAAAAAAAAAA=" | jq
{
  "hex": "0200000000101d5c9e7c85a8f8a2aa1cb3a9336be9e862f8e3b9cd0298c878b87c8dcf0609f740100
00000fefffff02f3959800000000160014c2b2b0aadb87fcd8fdca7605eb64e82dd0234fbc80969800000000
00160014cf8554fce63de1134ee1db77cf0cebcaa84ca0bb0247304402204ab49de6e3ef4bbbc77ee7ebb866e3f1
c36ea4de25a282daeb54d4387a9f025a02201efe73f618c3498a15c0eb134fd2a9be465972ea0ba79dfca2b73223
0f9b111e012103d8498fc24725096130e1f8563e407109439e2c9dd26264054833fa6cb2563f4900000000",
  "complete": true
}
g4WFT:HWI bitcoin$ bitcoin-cli sendrawtransaction 0200000000101d5c9e7c85a8f8a2aa1cb3a9336be
9e862f8e3b9cd0298c878b87c8dcf0609f740100000000fefffff02f3959800000000160014c2b2b0aadb87fc
d8fdca7605eb64e82dd0234fbc80969800000000160014cf8554fce63de1134ee1db77cf0cebcaa84ca0bb0247
304402204ab49de6e3ef4bbbc77ee7ebb866e3f1c36ea4de25a282daeb54d4387a9f025a02201efe73f618c3498a
15c0eb134fd2a9be465972ea0ba79dfca2b732230f9b111e012103d8498fc24725096130e1f8563e407109439e2c
9dd26264054833fa6cb2563f4900000000
297f570b6d05fe35fc18b16d1fd9654ea4df23be2c62c670a22a05de3d0bab0b
```

# The easy way[9]

```
>> bitcoind -signer=../HWI/hwi.py

   >> enumeratesigners

   >> signerfetchkeys

   >> signerdisplayaddress

   >> signerprocesspsbt

   >> signersend
```

[9] https://github.com/bitcoin/bitcoin/pull/14912

# The easy way

## `signersend`

» `signersend [{}] [{"DESTINATION": AMOUNT}]`
optionally specify input coins, fee, etc

» approve on device

» profit

# Signer protocol

- hardware wallets can sign stuff
- multisig services like BitGo can sign stuff
- standard interface to communicate with signers?
  - (Python) commands; or
  - JSON RPC
- WIP proposal[10] in PR 14912

[10] https://github.com/Sjors/bitcoin/blob/2018/11/rpc-signer/doc/external-signer.md

## `enumerate` (required)

Usage:

```
$ <cmd> enumerate
[
    {
        "fingerprint": "00000000"
    }
]
```

The command MUST return an (empty) array with at least a `fingerprint` field.

A future extension could add an optional return field with device capabilities. Perhaps a descriptor with wildcards. For example: `["pkh("44'/0'/$'/{0,1}/*"), sh(wpkh("49'/0'/$'/{0,1}/*")), wpkh("84'/0'/$'/{0,1}/*")]`. This would indicate the device supports legacy, wrapped SegWit and native SegWit. In addition it restricts the derivation paths that can used for those, to maintain compatibility with other wallet software. It also indicates the device, or the driver, doesn't support multisig.

A future extension could add an optional return field `reachable`, in case `<cmd>` knows a signer exists but can't currently reach it.

## `signtransaction` (required)

Usage:

```
$ <cmd> --fingerprint=<fingerprint> (--testnet) signtransaction <psbt>
base64_encode_signed_psbt
```

# Thanks

Slides: github.com/sjors/presentations

Blog: medium.com/provoost-on-crypto

PGP:

```
ED9B DF7A D6A5 5E23 2E84  5242 57FF 9BDB CC30 1009
```