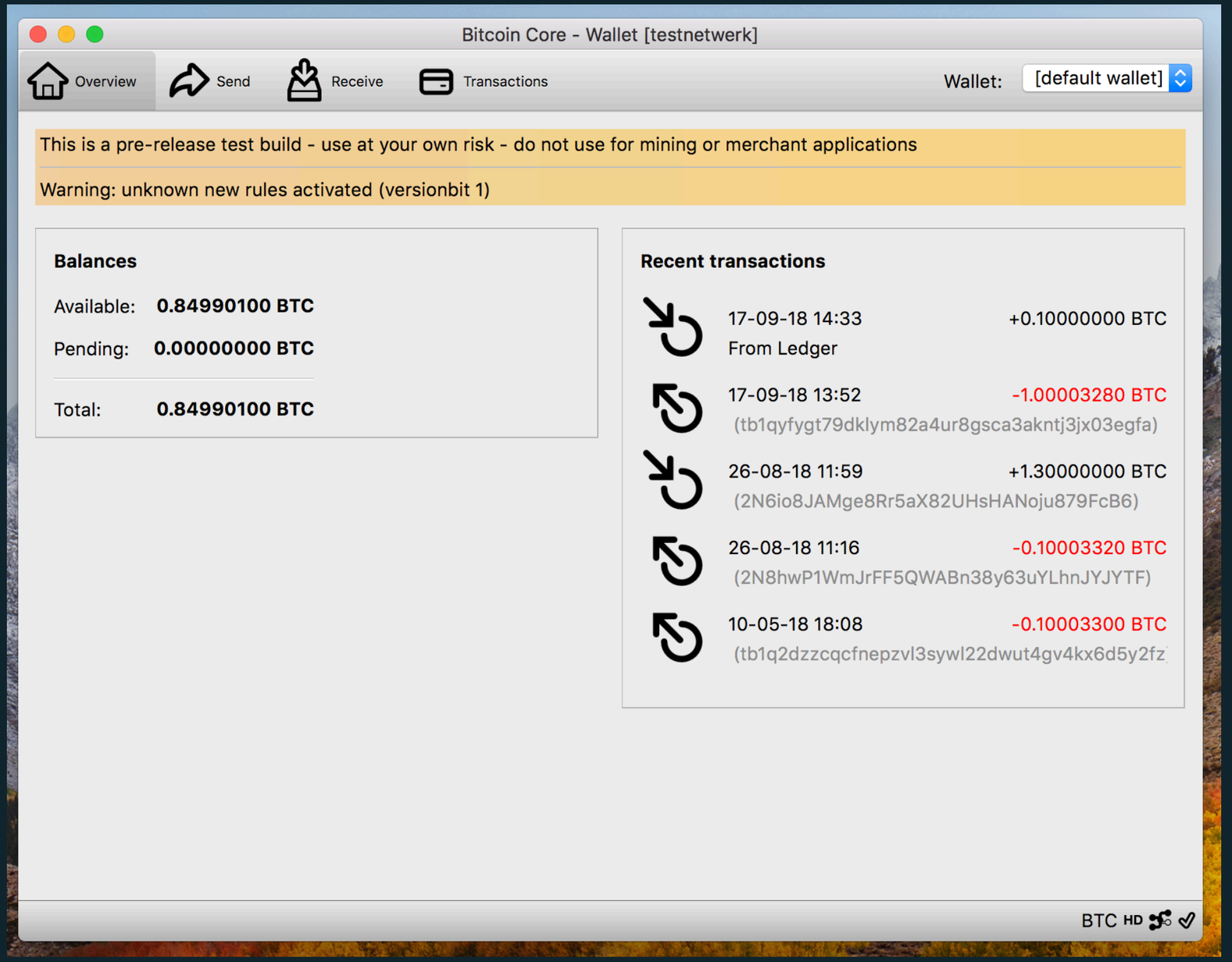
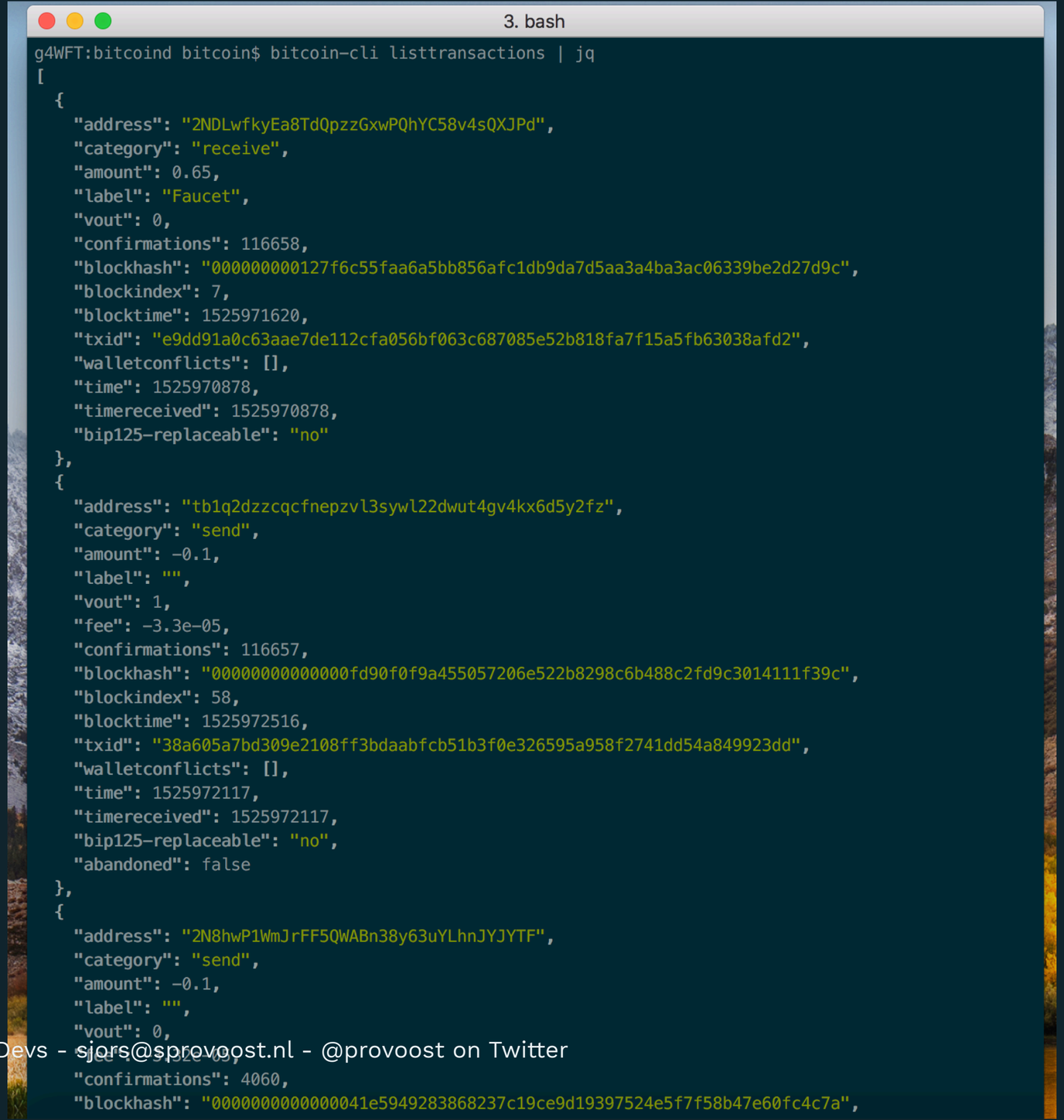
Bitcoin Core wallet

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": -3.3e-05,
"confirmations": 4060,
"blockhash": "000000000000041e5949283868237c19ce9d19397524e5f7f58b47e60fc4c7a",

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 code

Combined

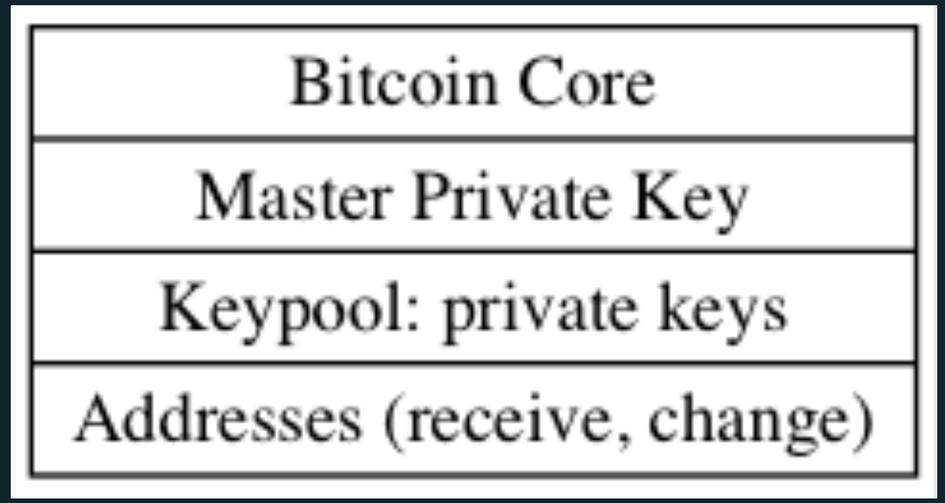
— keys not on your computer
— great privacy
— no external truth
— only hardware specific code to review

Problems

- how to encode transaction data? PSBT
- how to communicate between device and Core wallet:
  - Electrum Personal Server
  - Semi manually
  - JSON-RPC standard?
- minimize amount of stuff to install
- not too radical changes to Bitcoin Core

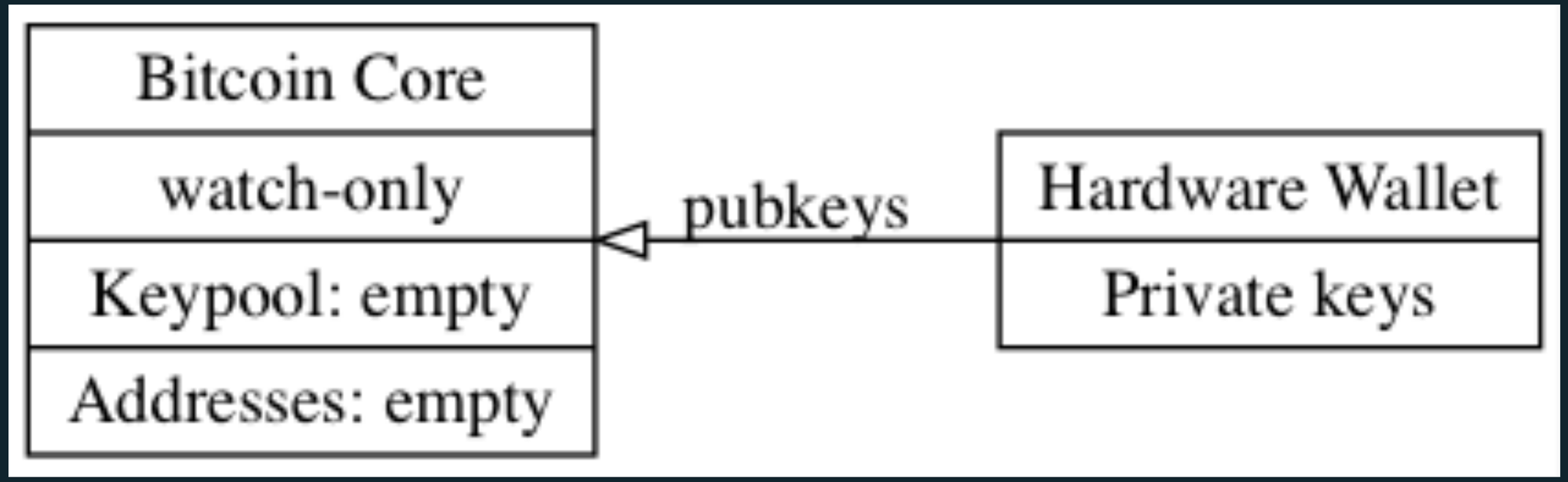
Anatomy of Bitcoin Core wallet

1. master private key
2. keypool of private keys
3. receive & change addresses



Core + HWW Setup

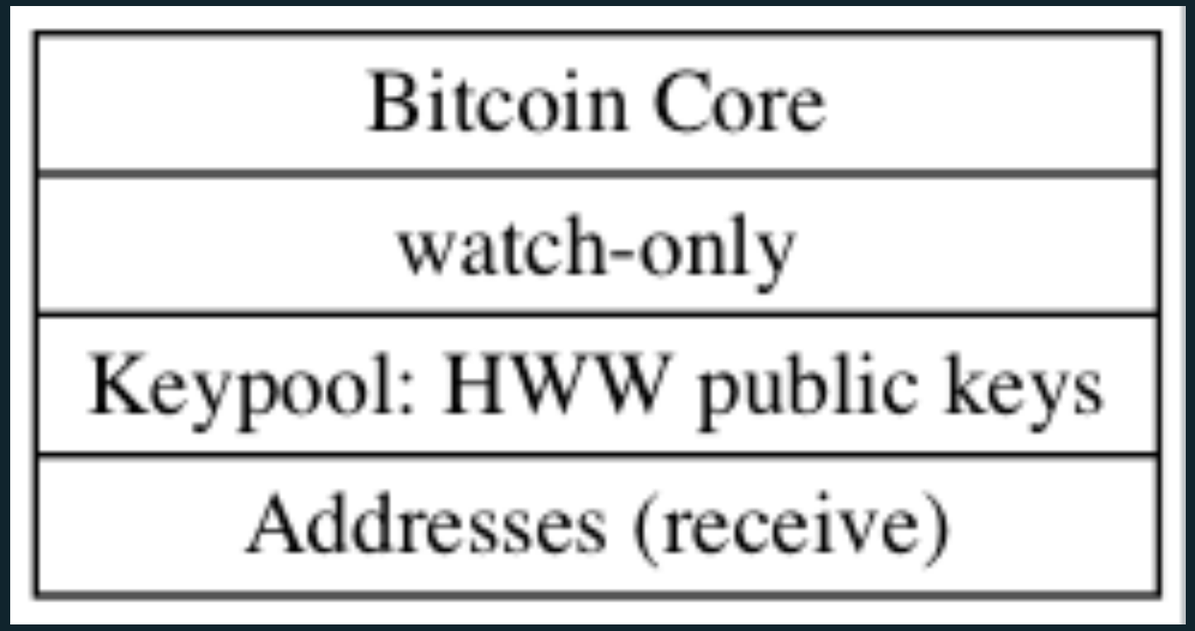
— Start with empty watch-only wallet
— Import public keys from device



Core + HWW Usage

— Fill keypool

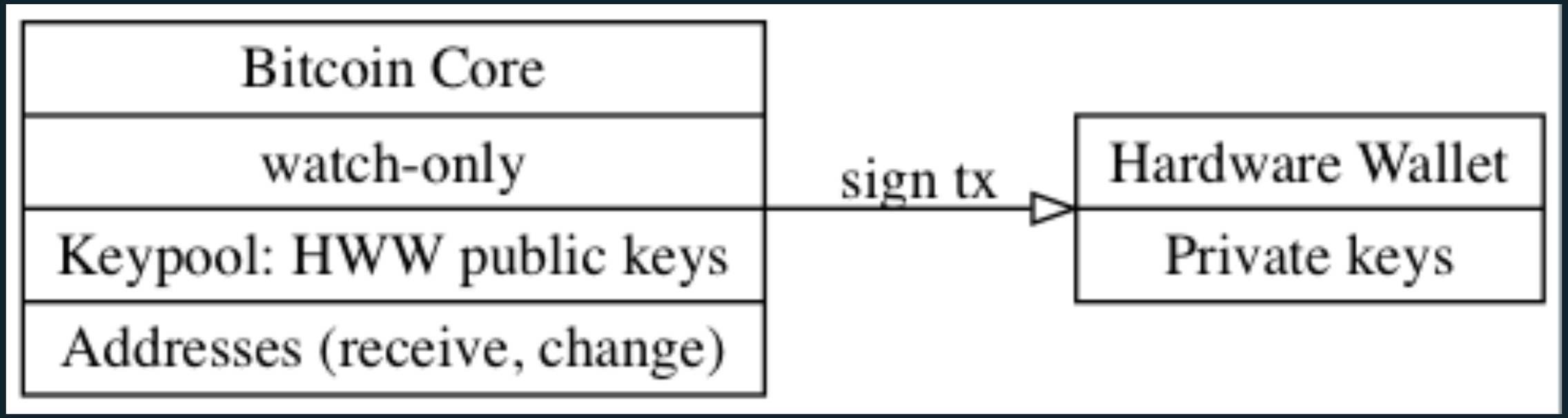
— Generate receive address



Core + HWW Usage

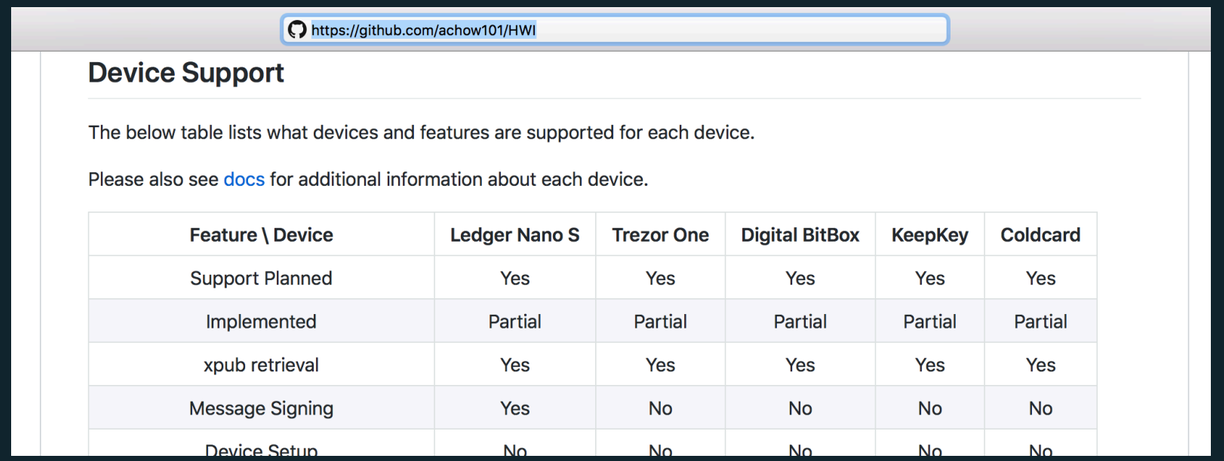
— Generate unsigned transaction in Core

— Sign on device



HWI

— Bitcoin Hardware Wallet Interaction scripts[0] by Andrew Chow (instructions[1])



[0] https://github.com/achow101/HWI

[1] https://gist.github.com/achow101/a9cf757d45df56753fae9d65db4d6e1d

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): needed for PSBT

Create watch-only wallet

```
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
}
```

Usefull stuff added in v0.17.0:

— dynamic wallet create / load / unload

— watch-only wallets

Get keys from device: receive

```
g4WFT:HWI bitcoin$ ./hwi.py --testnet --fingerprint d9d676d4 getkeypool "m/84'/1'/0'/0" 0 0 --keypool
| jq
[
  {
    "pubkeys": [
      {
        "03d8498fc24725096130e1f8563e407109439e2c9dd26264054833fa6cb2563f49": {
          "0000000000000000000000000000000d476d6d9": "m/84h/1h/0h/0/0"
        }
      }
    ],
    "scriptPubKey": {
      "address": "mzSDtqBfL3GziGZaWkBC3YPR5KFqBgQ4Uw"
    },
    "timestamp": "now",
    "internal": false,
    "keypool": true
```

Get keys from device: change

```
g4WFT:HWI bitcoin$ ./hwi.py --testnet --fingerprint d9d676d4 getkeypool "m/84'/1'/0'/1" 0 0 --keypool
--internal | jq
[
  {
    "pubkeys": [
      {
        "028f352e8bfe664ca4def97561fa35e0b8068964bd2a7a8c2651ce218f01fe6b87": {
          "0000000000000000000000000000000d476d6d9": "m/84h/1h/0h/1/0"
        }
      }
    ],
    "scriptPubKey": {
      "address": "myGRSsjB6WWjJ89R4EFZWSTpYJzASvK2F1"
    },
    "timestamp": "now",
    "internal": true,
    "keypool": true
```

Import keys into wallet

— Use achow101 branch[2] (until it's merged)

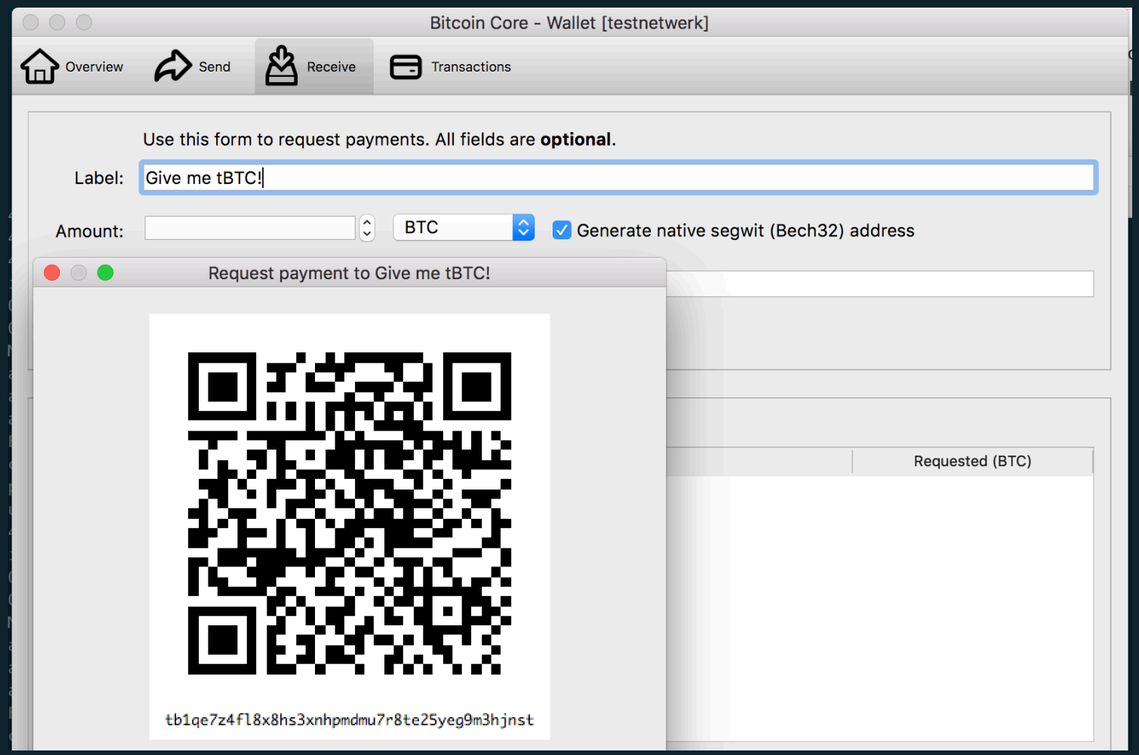
— import lots of keys so you never have to repeat this

```
g4WFT:HWI bitcoin$ bitcoin-cli -rpcwallet=ledger importmulti '[{"pubkeys": [{"028f352e8bfe664ca4def975
61fa35e0b8068964bd2a7a8c2651ce218f01fe6b87": {"00000000000000000000000000000000d476d6d9": "m/84h/1h/0h
/1/0"}}], "scriptPubKey": {"address": "myGRSsjB6WWjJ89R4EFZWSTpYJzASvK2F1"}, "timestamp": "now", "inte
rnal": true, "keypool": true}]' | jq
[
  {
    "success": true
  }
]
```

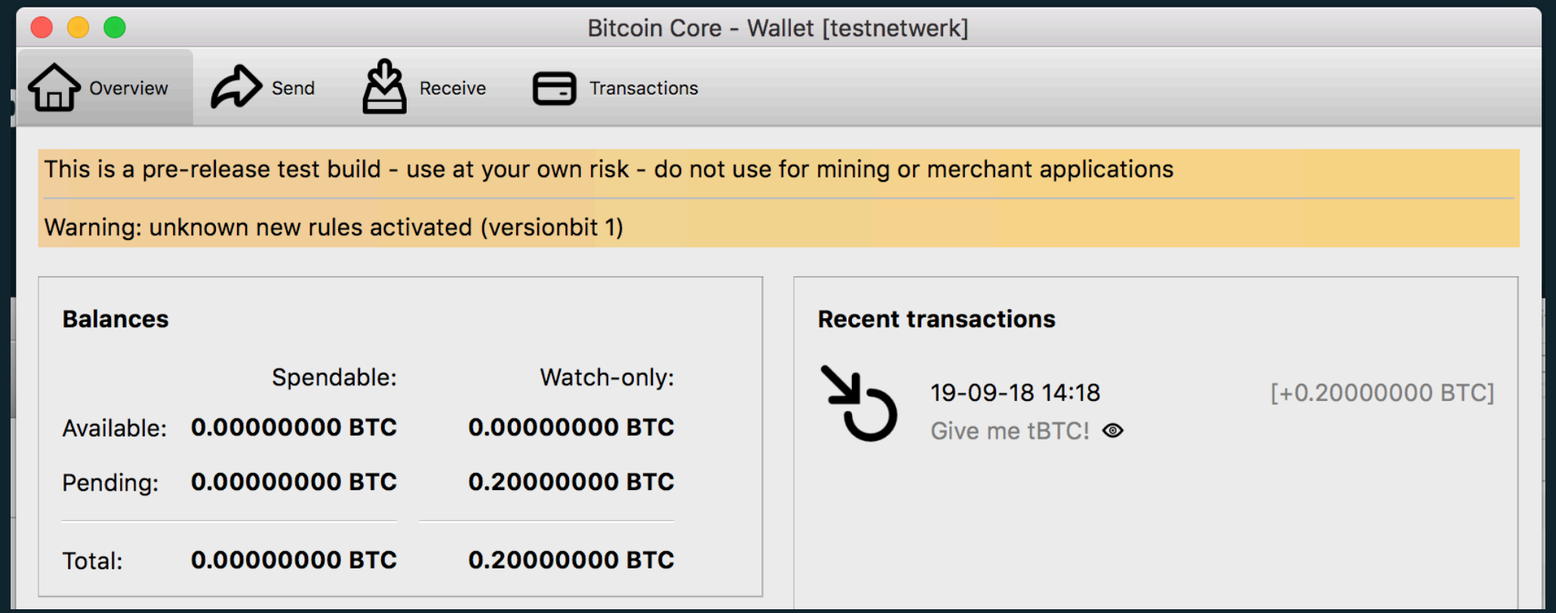
[2] https://github.com/achow101/bitcoin/tree/hww

Generate receive address

— no hardware device needed!



Wait for confirmation



— there's a PR[4] to make this prettier

[4] https://github.com/bitcoin/bitcoin/pull/13966

Prepare transaction

```
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/muHGNnWdtRUAACAAQAAgAAAAIABAAAAAAAAAAAAIgIDPU8aMJAgXoQPyn6E7LrLc/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

```
g4WFT:HWI bitcoin$ bitcoin-cli -rpcwallet=ledger decodepsbt "cHNidP8BAHECAAAAAdXJ58haj4oqocs
6kza+noYvjjuc0CmMh4uHyNzwYJ90AQAAAAD+////AvOVmAAAAAAAFgAUwrKwqtuH/Nj9ynYF62ToLdAjT7yAlpgAAAA
AABYAFM+FVPzmPeETTuHbd88M68qoTKC7AAAAAAABAR8ALTEBAAAAABYAFM+FVPzmPeETTuHbd88M68qoTKC7IgYD2Em
PwkclCWEw4fhWPkBxCUOeLJ3SYmQFSDP6bLJWP0kY2dZ21FQAAIABAACAAAAAgAAAAAAAAAAAACICAo81Lov+Zkyk3vl
1Yfo14LgGiWS9KnqMJlHOIY8B/muHGNnWdtRUAACAAQAAgAAAAIABAAAAAAAAAAAAiAgPYSY/CRyUJYTDh+FY+QHEJQ54
sndJiZAVIM/psslY/SRjZ1nbUVAAAgAEAAIAAAACAAAAAAAAAAAA" | jq
{
  "tx": {
    "txid": "297f570b6d05fe35fc18b16d1fd9654ea4df23be2c62c670a22a05de3d0bab0b",
    "hash": "297f570b6d05fe35fc18b16d1fd9654ea4df23be2c62c670a22a05de3d0bab0b",
    "version": 2,
    "size": 113,
    "vsize": 113,
    "weight": 452,
    "locktime": 0,
    "vin": [
      {
        "txid": "749f60f0dcc8878b878c29d09c3b8e2f869ebe36933acba12a8a8f5ac8e7c9d5",
        "vout": 1,
        "scriptSig": {
          "asm": "",
          "hex": ""
        },
        "sequence": 4294967294
      }
    ],
```

```
  "vout": [
    {
      "value": 0.09999859,
      "n": 0,
      "scriptPubKey": {
        "asm": "0 c2b2b0aadb87fcd8fdca7605eb64e82dd0234fbc",
        "hex": "0014c2b2b0aadb87fcd8fdca7605eb64e82dd0234fbc",
        "reqSigs": 1,
        "type": "witness_v0_keyhash",
        "addresses": [
          "tb1qc2etp2kmsl7d3lw2wcz7ke8g9hgzxnau8hasq7"
        ]
      }
    },
    {
      "value": 0.1,
      "n": 1,
      "scriptPubKey": {
        "asm": "0 cf8554fce63de1134ee1db77cf0cebcaa84ca0bb",
        "hex": "0014cf8554fce63de1134ee1db77cf0cebcaa84ca0bb",
        "reqSigs": 1,
        "type": "witness_v0_keyhash",
        "addresses": [
          "tb1qe7z4fl8x8hs3xnhpmdmu7r8te25yeg9m3hjnst"
        ]
      }
    }
  ]
},
"unknown": {},
```

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

```
"outputs": [
  {
    "bip32_derivs": [
      {
        "pubkey": "028f352e8bfe664ca4def97561fa35e0b8068964bd2a7a8c2651ce218f01fe6b87",
        "master_fingerprint": "d9d676d4",
        "path": "m/84'/1'/0'/1/0"
      }
    ]
  },
```

Sign transaction


```
g4WFT:HWI bitcoin$ ./hwi.py --testnet --fingerprint d9d676d4 signtx cHNidP8BAHECAAAAAdXJ58haj4oqocs6kza+noYvjjuc0CmMh4uHyNzwYJ90AQAAAAD+////AvOVmAAAAAAAFgAUwrKwqtuH/Nj9ynYF62ToLdAjT7yAlpgAAAAAABYAFM+FVPzmPeETTuHbd88M68qoTKC7AAAAAAAABAR8ALTEBAAAAABYAFM+FVPzmPeETTuHbd88M68qoTKC7IgYD2EmPwkclCWEw4fhWPkBxCUOeLJ3SYmQFSDP6bLJWP0kY2dZ21FQAAIABAACAAAAAgAAAAAAAAAAAACICAo81Lov+Zkyk3vl1Yfo14LgGiWS9KnqMJlHOIY8B/muHGNnWdtRUAACAAQAAgAAAAIABAAAAAAAAAAAiAgPYSY/CRyUJYTDh+FY+QHEJQ54sndJiZAVIM/psslY/SRjZ1nbUVAAAgAEAAIAAAACAAAAAAAAAAAA
{"psbt": "cHNidP8BAHECAAAAAdXJ58haj4oqocs6kza+noYvjjuc0CmMh4uHyNzwYJ90AQAAAAD+////AvOVmAAAAAAAFgAUwrKwqtuH/Nj9ynYF62ToLdAjT7yAlpgAAAAAABYAFM+FVPzmPeETTuHbd88M68qoTKC7AAAAAAAABAR8ALTEBAAAAABYAFM+FVPzmPeETTuHbd88M68qoTKC7IgID2EmPwkclCWEw4fhWPkBxCUOeLJ3SYmQFSDP6bLJWP0lHMEQCIEq0nebj70u7x37n67hm4/HDbqTeJaKC2utU1Dh6nwJaAiAe/nP2GMNJihXA6xNP0qm+Rlly6gunnfyitzIjD5sRHgEiBgPYSY/CRyUJYTDh+FY+QHEJQ54sndJiZAVIM/psslY/SRjZ1nbUVAAAgAEAAIAAAACAAAAAAAAAAAAAIgICjzUui/5mTKTe+XVh+jXguAaJZL0qeowmUc4hjwH+a4cY2dZ21FQAAIABAACAAAAAgAEAAAAAAAAACICA9hJj8JHJQlhMOH4Vj5AcQlDniyd0mJkBUgz+myyVj9JGNnWdtRUAACAAQAAgAAAAIAAAAAAAAAAAAA="}
```

Before

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

After


```
"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"
        }
      ]
    }
  ],
```

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": "02000000000101d5c9e7c85a8f8a2aa1cb3a9336be9e862f8e3b9cd0298c878b87c8dcf0609f740100
000000feffffff02f39598000000000160014c2b2b0aadb87fcd8fdca7605eb64e82dd0234fbc80969800000000
00160014cf8554fce63de1134ee1db77cf0cebcaa84ca0bb0247304402204ab49de6e3ef4bbbc77ee7ebb866e3f1
c36ea4de25a282daeb54d4387a9f025a02201efe73f618c3498a15c0eb134fd2a9be465972ea0ba79dfca2b73223
0f9b111e012103d8498fc24725096130e1f8563e407109439e2c9dd26264054833fa6cb2563f4900000000",
  "complete": true
}
g4WFT:HWI bitcoin$ bitcoin-cli sendrawtransaction 02000000000101d5c9e7c85a8f8a2aa1cb3a9336be
9e862f8e3b9cd0298c878b87c8dcf0609f740100000000feffffff02f39598000000000160014c2b2b0aadb87fc
d8fdca7605eb64e82dd0234fbc80969800000000160014cf8554fce63de1134ee1db77cf0cebcaa84ca0bb0247
304402204ab49de6e3ef4bbbc77ee7ebb866e3f1c36ea4de25a282daeb54d4387a9f025a02201efe73f618c3498a
15c0eb134fd2a9be465972ea0ba79dfca2b732230f9b111e012103d8498fc24725096130e1f8563e407109439e2c
9dd26264054833fa6cb2563f4900000000
297f570b6d05fe35fc18b16d1fd9654ea4df23be2c62c670a22a05de3d0bab0b
```

Signer RPC

WIP, perhaps one day a BIP?

— hardware wallets can sign stuff
— multisig services like BitGo can sign stuff
— a JSON-RPC for wallets to communicate with signers?

Hardware wallet side:

```
enumerate
getxpub "device_id" "bip32_path"
displayaddress "device_id" "bip32_path" ("address_type")
signtx "psbt"
```

Bitcoin Core side:

```
bitcoind -signerrpc=localhost:1000

listsigners
displayaddress "device_id" "bip32_path" ("address_type")
importsignerkeypool "device_id" "bip32_path" start end
sendto "address" {signer: "device_id"}
```

Thanks

Slides: slideshare.net/provoost

Blog: medium.com/provoost-on-crypto

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