Basic Bitcoin Tech: Connecting a Wallet

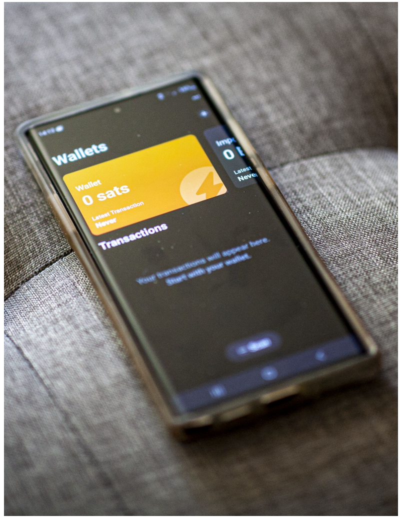
Host - Simplest Bitcoin Book w/ Portland.HODL

- Overview -

Topics

- What is a transaction?
- Connecting a wallet your node
  - Watch Only
  - Signing a transaction
- How to verify a transaction

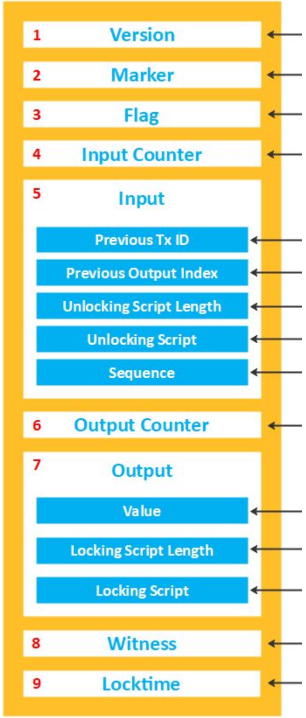
What is a Bitcoin transaction?



Definition

- “A transaction is when participant A signs over a designated amount of Bitcoin they own to participant B”
- The sender must have all the required signatures to send the funds to the receiver.
- Without the signatures the transaction is invalid and funds wont move from one address to another.

Transaction Structure



1 Version

2 Marker

3 Flag

4 Input Counter

5 Input

- Previous Tx ID
- Previous Output Index
- Unlocking Script Length
- Unlocking Script
- Sequence

6 Output Counter

7 Output

- Value
- Locking Script Length
- Locking Script

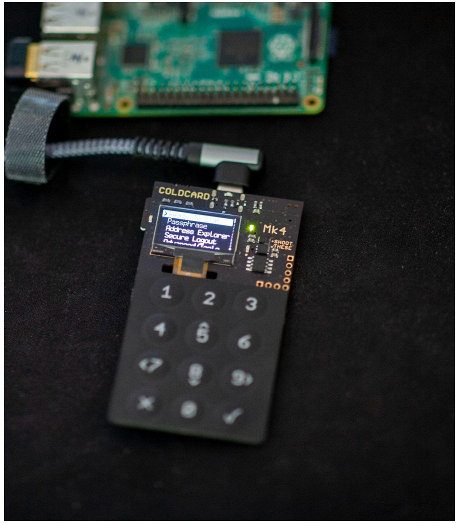
8 Witness

9 Locktime

Notes about transactions

- Transactions move through 3 main stages
  - Broadcast
  - Mempool
  - Mined into a block
- Transactions must be properly signed to move bitcoin
- Transactions can have multiple senders or receivers (possibly both)
- Transactions always have to pay a fee to the miners for their work
  - The fee is the difference between the input value and the output value
- A transaction is comprised of inputs (UTXO’s)
- A transaction is data that must be broadcast to the network through a node.

Linking your wallet to your node.

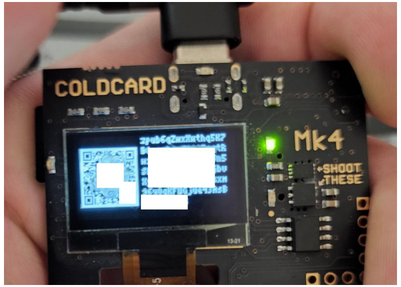


There are 2 primary use cases for connecting your wallet to your node.

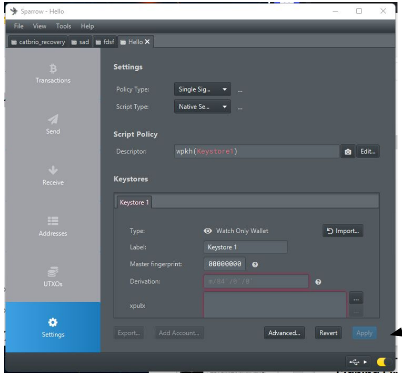
- **Watch only** : Keep track of funds and generate new addresses. The private key stays air gapped and funds are not spendable (The XPUB is imported)
- **Signing :** The wallet is connected to the node in such a way funds can be spent (USB, SD-Card, NFC). Some examples of this are Coldcard and Electrum over USB, Ledger Live, and Trezor Suite.

Watch Only Link - No Spending

Cold Card QR (XPUB)



Sparrow XPUB Import



Settings

Policy Type: Single Sig...

Script Type: Native Se...

Script Policy

Descriptor: wpkh(Keystore1)

Keystores

Keystore 1

Type: Watch Only Wallet

Label: Keystore 1

Master fingerprint: 00000000

Derivation: m/84'/0'/0'

xpub:

A watch only link is a link to a node where an XPUB (extended public key) or a HD (Hierarchical Descriptor) wallet are imported and the node keeps track of balances and can generate new addresses.

Some wallets accept XPUBs (such as blue wallet and Sparrow) - Others can accept files such a Bitcoin Core and Electrum

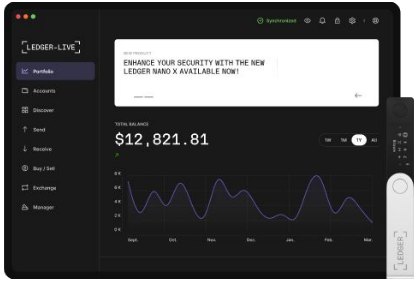
One of the biggest advantages to linking your wallet to your node is that you can verify and validate transactions trustlessly. That means you do not need to use a block explorer (someone else's node) to verify that your funds have arrived.

Connected to 3rd Party Node BAD!!!

Signing Link - Spendable Transactions

- There are multiple ways to connect a wallet to your node to sign transactions.
  - Linking over USB
  - SD Card
  - Import Seed Phrase (This is creating another wallet)
- Important to ensure the wallet software you are using actually connects to your node and **not to** a third parties' node.
- Breaking the airgap potentially can expose keys if the device is compromised.
- Hardware wallet must be 'unlocked to spend funds' watch only works all the time.

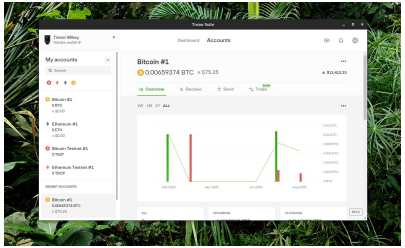
Ledger Live - Can connect to your full node



ENHANCE YOUR SECURITY WITH THE NEW LEDGER NANO X AVAILABLE NOW!

$12,821.81

Trezor Suite Can connect to your full node w/ Electrum Server



Trevor Wikey
Hidden wallet #

Bitcoin #1
0.00659374 BTC ≈ $75.25
$11,412.23

Bitcoin #1
0 BTC
≈ $0.00

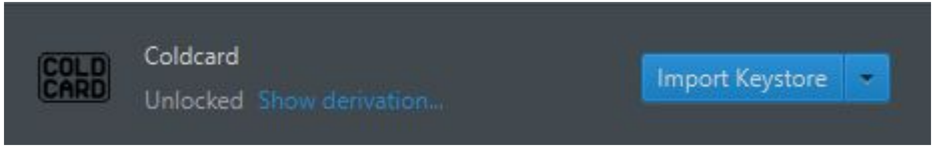
Ethereum #1
0 ETH
≈ $0.00

Bitcoin Testnet #1
0 TEST

Ethereum Testnet #1
0 TROP

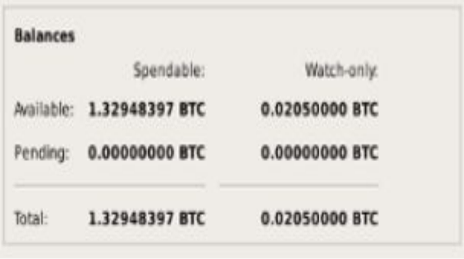
Bitcoin #1
0.00659374 BTC
≈ $75.25

Cold Card Needs to use a external software Bitcoin Core or Sparrow Directly.



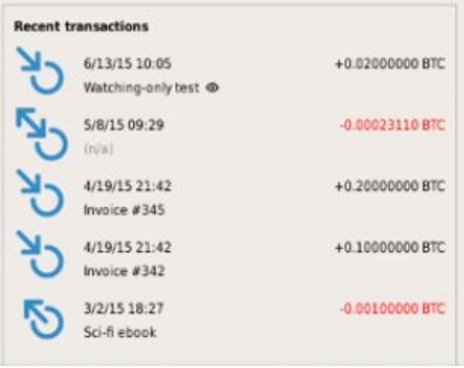
Verifying a transaction!

Verify your funds with your own full node!



Balances

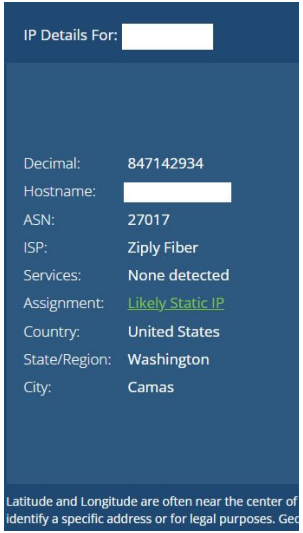
	Spendable:	Watch-only:
Available:	1.32948397 BTC	0.02050000 BTC
Pending:	0.00000000 BTC	0.00000000 BTC
Total:	1.32948397 BTC	0.02050000 BTC



Recent transactions

6/13/15 10:05 Watching-only test	+0.02000000 BTC
5/8/15 09:29 (n/a)	-0.00023110 BTC
4/19/15 21:42 Invoice #345	+0.20000000 BTC
4/19/15 21:42 Invoice #342	+0.10000000 BTC
3/2/15 18:27 Sci-fi ebook	-0.00100000 BTC

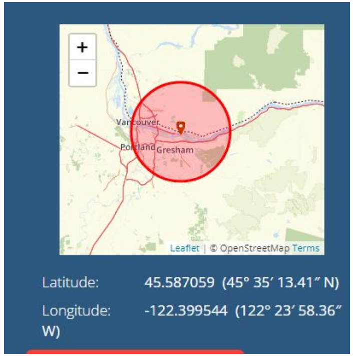
- Verifying a transaction means that ‘you’ know with full certainty that funds are in your custody or have been received by the other party.
- When your XPUB or wallet is connected to your node you can with certainty know that a transaction has settled.
- The wallet software will show an up-to-date balance.
- If you want to go a step further you can check in the Bitcoin Core command line. ‘gettransaction (txid)’



IP Details For: [redacted]

Decimal:	847142934
Hostname:	[redacted]
ASN:	27017
ISP:	Ziply Fiber
Services:	None detected
Assignment:	Likely Static IP
Country:	United States
State/Region:	Washington
City:	Camas

Latitude and Longitude are often near the center of
identify a specific address or for legal purposes. Ge



Latitude:	45.587059 (45° 35′ 13.41″ N)
Longitude:	-122.399544 (122° 23′ 58.36″ W)

Broadcasting a Transaction (TX)

- To spend bitcoin - a signed transaction must make it to the miners.
- To do this 99.99999% of people broadcast a transaction to the Bitcoin network with an internet connected computer.
- These transactions if they are segwit can't be manipulated but the act of broadcasting the TX can expose your IP Address if you aren't using TOR or a VPN & even then this doesn't ensure perfect privacy.
- It does ensure that your IP address isn't leaked.

- If you use a hardware wallet with an SD Card or the ability to export a transaction, you can then go to another computer that wouldn't expose personal information and then broadcast a transaction from that device. *E.g. Using a library computer with sparrow wallet.*

Thanks For Listening.

1. Questions or Comments? Please ask to come on stage.
2. Anything incorrect please comment on the slide in question.