Current state and the future of wallets
Privacy
Transaction / scripts privacy

Security
Keystorage
Cold-Storage

Trust
No-trust required
Chain-Validation
Consensus
Trust
Privacy
Security
Scripts sharing
Central validation
No control over keys
Trust
Privacy
Security

- Scripts sharing
- Missing cold storage
- SPV validation

Electrum
Centralized validation
Current state:

New/novice users *tend* to use centralised validation.
Current state:

New/novice users tend to use centralised validation.

- Required validation device
- Validation lead time
- Bandwidth and CPU requirements
Centralized validation in practice

- \(~200\text{GB+ disk space}\) (large indexes)
- Heavy disk I/O through indexing
- **Full validation** „underneath“ (Bitcoin Core)
Downsides of centralized validation

- **Fake** transactions / transaction omission
- **No control over the** consensus layer
- Abandons **privacy** completely
Advantages of centralized validation

✓ Immediately ready to use
✓ Fast wallet recovery
✓ Very low bandwidth costs
✓ Can serve large amount of wallets
Centralized key-storage
✓ No security setup required
× „Owns“ no Bitcoins
× „Owns“ only the right to eventually access and move Bitcoins

Users are often not aware!
8. Simplified Payment Verification

It is possible to verify payments without running a full network node. A user only needs to keep a copy of the block headers of the longest proof-of-work chain, which he can get by querying network nodes until he's convinced he has the longest chain, and obtain the Merkle branch linking the transaction to the block it's timestamped in. He can't check the transaction for himself, but by linking it to a place in the chain, he can see that a network node has accepted it, and blocks added after it further confirm the network has accepted it.
SPV

- Verify headers ✅
- Can check some consensus rules ✅
- Weak 0-conf handling ❌
- Network "leeches" ❌
- Rely on a "free service" ❌
- Fee estimation is probably impossible ❌
- Often rely on DNS seeds ❌
SPV

Acceptable Bandwidth consumption

Acceptable amount of decentralization
SPV

privacy?
<table>
<thead>
<tr>
<th>SPV privacy</th>
<th>BIP37 - Bloom Filters</th>
<th>Electrum SPV</th>
<th>BIP158 - Compact Block Filters</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>✓ Low bandwidth</td>
<td>✓ Low bandwidth</td>
<td>✓ „more“ bandwidth</td>
</tr>
<tr>
<td>✓</td>
<td>✓ Can filter mempool</td>
<td>✓ MITM protection through SSL</td>
<td>✓ Privacy (?)</td>
</tr>
<tr>
<td>×</td>
<td>× No privacy</td>
<td>× (No privacy)</td>
<td>✓ Widely useful filter structures</td>
</tr>
<tr>
<td>×</td>
<td>× Personal filtering</td>
<td>× Personal filtering</td>
<td>✓ Committable through soft-fork</td>
</tr>
<tr>
<td>(incentive model)</td>
<td>(incentive model)</td>
<td>(incentive model)</td>
<td>× not (widely) deployed</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>× no (useful) technique to filter mempool</td>
</tr>
</tbody>
</table>
SPV privacy

Full block SPV

X „high“ bandwidth costs
✓ Can „migrate“ to full validation
✓ Privacy
✓ Reduced consensus checks
understanding **SPV** filtering

**BIP37** - Bloom Filters

Filters transactions for the client

RELEVANT TRANSACTIONS (FALSE POSITIVES)
Understanding SPV filtering

BIP37 - Bloom Filters

SPV BF

Bloom Filter

Internet Traffic

Men in the Middle
ISP, WIFI PROVIDER, STATE ACTORS

Relevant Transactions (False Positives)

Peer with NODE_BLOOM

Filters transactions for the client
understanding **SPV** filtering

**BIP158** - Client Side Filtering

Client finds relevant Blocks

NODE SUPPORTING BIP158

**SPV BF**

**BLOCK FILTERS**

**BLOCKS**
understanding **SPV** filtering

**BIP158** - Client Side Filtering

144 blocks \( \approx \) 144MB

- Filtersize: \( \approx 2\% \)

1 day \( = \) \( \approx \) 2.88MB

30 days \( = \) \( \approx \) 86.4 MB

7 days \( = \) \( \approx \) 20.16 MB

90 days \( = \) \( \approx \) 259.2 MB
understanding SPV filtering

FULL BLOCK / HYBRID

144 blocks \(\approx\) 144MB

1 day = \(~144\text{MB}\)
30 days = \(~4.32\text{ GB}\)
7 days = \(~1'008\text{ MB}\)
90 days = \(~12.96\text{ GB}\)
Decentralization

Resource costs

Centralized validation solutions

SPV

Electrum (SPV)

Core / full node
FUTURE OF WALLETS?
Privacy
Transaction / scripts privacy

Security
Keystorage
Cold-Storage

Trust
No-trust required
Chain-Validation
Consensus / p2p
Catching up a month of blocks
(45min; consumer system)

Acceptable CPU / memory rates once in-sync

<table>
<thead>
<tr>
<th>Prozessname</th>
<th>% CPU</th>
<th>Physikal. Speicher</th>
<th>CPU-Zeit</th>
<th>Threads</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slack Helper</td>
<td>0.4</td>
<td>156.9 MB</td>
<td>2:11.66</td>
<td>5</td>
</tr>
<tr>
<td>Bitcoin Core</td>
<td>0.4</td>
<td>1.13 GB</td>
<td>1:10:15.74</td>
<td>18</td>
</tr>
<tr>
<td>Slack Helper</td>
<td>0.3</td>
<td>315.3 MB</td>
<td>9:22.91</td>
<td>20</td>
</tr>
<tr>
<td>Slack Helper</td>
<td>0.2</td>
<td>155.2 MB</td>
<td>25.60</td>
<td>20</td>
</tr>
<tr>
<td>Slack</td>
<td>0.2</td>
<td>86.4 MB</td>
<td>4:32.27</td>
<td>30</td>
</tr>
<tr>
<td>Slack Helper</td>
<td>0.1</td>
<td>74.4 MB</td>
<td>24.13</td>
<td>20</td>
</tr>
<tr>
<td>Slack Helper</td>
<td>0.0</td>
<td>61.2 MB</td>
<td>7.04</td>
<td>19</td>
</tr>
</tbody>
</table>
Hybrid SPV

Sync and check **headers**

Download **relevant** blocks (use BIP158)

Use **SPV**

**Wallet is ready to use**

Download **missing** blocks

**Full-Validation**

**Upgrade** transactions once they are fully validated
Privacy and self-verification (no trust) is not an opt-in model
Keep users **away** from trusted third parties
UTXO set commitments

{
  "height": 530075,
  "bestblock": "0000000000000000002fe10af166937d506ece7fad4381fda6cb86e9e1404be2",
  "transactions": 24567998,
  "txouts": 50460119,
  "bogosize": 3798659787,
  "hash_serialized_2": "090c1276fe42f98246840fabac42dfa0e8b89b428f81ab16d53d69ae669bec4b",
  "disk_size": 2921681465,
  "total_amount": 17125767.33401612
}

BIP 174

Partially Signed Bitcoin Transaction Format (PSBT)
**Fundrawtransaction**

(Enforce **WatchOnly**)  
Multiwallet

Dynamic creation and loading of wallets

**PROXY BRIDGE**

(Scan **TxOutSet**)

- **HTTPS**
- **TOR**
- **STRATUM (TCP/TLS)**

**NODE_NETWORK_LIMITED**
### JoinMarket Orderbook

18 orders found by 11 counterparties

<table>
<thead>
<tr>
<th>Type</th>
<th>Counterparty</th>
<th>Order ID</th>
<th>Fee</th>
<th>Minor Fee Contribution / BTC</th>
<th>Minimum Size / BTC</th>
<th>Maximum Size / BTC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Absolute Fee</td>
<td>J5EawiYMqgc77Gk</td>
<td>0</td>
<td>0.00000202</td>
<td>0.00000000</td>
<td>0.00100000</td>
<td>0.05455444</td>
</tr>
<tr>
<td>Absolute Fee</td>
<td>J5AEGMk9WzmJcG6L</td>
<td>0</td>
<td>0.00000046</td>
<td>0.00000000</td>
<td>0.00273000</td>
<td>0.0378056</td>
</tr>
<tr>
<td>Absolute Fee</td>
<td>J57RC7fh3M9Xq2g</td>
<td>1</td>
<td>0.00000854</td>
<td>0.00000000</td>
<td>0.07358091</td>
<td>0.17257333</td>
</tr>
<tr>
<td>Absolute Fee</td>
<td>J5AEGMk9WzmJcG6L</td>
<td>1</td>
<td>0.00001351</td>
<td>0.00000000</td>
<td>0.03768057</td>
<td>0.05446864</td>
</tr>
<tr>
<td>Absolute Fee</td>
<td>J5x2a2CTwVhKmR2YFR</td>
<td>0</td>
<td>0.00005000</td>
<td>0.00000000</td>
<td>0.10000000</td>
<td>0.22497598</td>
</tr>
<tr>
<td>Absolute Fee</td>
<td>J57RC7fNh3M9Xq2g</td>
<td>0</td>
<td>0.00005420</td>
<td>0.00000000</td>
<td>0.00273000</td>
<td>0.07358090</td>
</tr>
<tr>
<td>Relative Fee</td>
<td>J5AEGMk9WzmJcG6L</td>
<td>2</td>
<td>0.00010063</td>
<td>0.00000000</td>
<td>0.30446865</td>
<td>1.46144594</td>
</tr>
<tr>
<td>Relative Fee</td>
<td>J57RC7fNh3M9Xq2g</td>
<td>2</td>
<td>0.00032723</td>
<td>0.00000000</td>
<td>0.17257354</td>
<td>0.66258490</td>
</tr>
<tr>
<td>Relative Fee</td>
<td>J58SSN27fM7NwWyp</td>
<td>0</td>
<td>0.0007%</td>
<td>0.00000000</td>
<td>2.14265714</td>
<td>4.16541954</td>
</tr>
<tr>
<td>Relative Fee</td>
<td>J5Exvdkf09Dh6kln</td>
<td>0</td>
<td>0.0045%</td>
<td>0.00000000</td>
<td>0.01000000</td>
<td>1.5590720</td>
</tr>
<tr>
<td>Relative Fee</td>
<td>J59a2ajbXcX4D6r7</td>
<td>1</td>
<td>0.005%</td>
<td>0.00000000</td>
<td>0.01000000</td>
<td>9.99999999</td>
</tr>
<tr>
<td>Relative Fee</td>
<td>J59e6B6uUXFxed1</td>
<td>0</td>
<td>0.009%</td>
<td>0.00000000</td>
<td>0.10666666</td>
<td>17.10377123</td>
</tr>
<tr>
<td>Relative Fee</td>
<td>J5Dq1NHr77j1upRw</td>
<td>0</td>
<td>0.018%</td>
<td>0.00000000</td>
<td>0.03800000</td>
<td>1.88143549</td>
</tr>
<tr>
<td>Relative Fee</td>
<td>J5EphFt276G96xqFs</td>
<td>0</td>
<td>0.02%</td>
<td>0.00000000</td>
<td>0.07500000</td>
<td>6.62622558</td>
</tr>
<tr>
<td>Relative Fee</td>
<td>J5ScWFMk6gdsx29F6</td>
<td>0</td>
<td>0.02%</td>
<td>0.00000000</td>
<td>0.07500000</td>
<td>0.28283752</td>
</tr>
<tr>
<td>Relative Fee</td>
<td>J58t2ajX6XITC6h8u7</td>
<td>2</td>
<td>0.02%</td>
<td>0.00000000</td>
<td>10.00000000</td>
<td>26.90899999</td>
</tr>
</tbody>
</table>
WALLET OF THE FUTURE

MULTIPLE FACTORS
(HARDWARE WALLET)
MULTISIG BY DEFAULT

OWN VALIDATION
USE CPU & BANDWIDTH WHEN AVAILABLE

OWN FEE ESTIMATIONS

PRIVACY FEATURES
CoinJoins
Broadcast obfuscation

INTEGRATED L2

EASY TO USE

REL IABLE BACKUP SOLUTION

MIXED HARDWARE SOFTWARE SOLUTION
Thanks, Q&A?

dev@jonasschnelli.ch
PGP: CA1A2908DCE2F13074C62CDE1EB776BB03C7922D

_jonasschnelli_

github.com/jonasschnelli