Random BDK Stuff

Alekos Filini @ Satoshi Spritz Live

Topics Covered

- From policy to working wallet
- BIP157/158 sync

Complex Spending Policies

- Use the potential of Bitcoin scripts
  - Mix multiple keys, hash/preimages, timelocks...
- Writing scripts manually is hard
  - Sipa and Andrew invent Miniscript

Miniscript

- High level language to describe spending policies
- Only a few operands:
  - pk(), sha256(), hash256(), ripemd160(), hash160()
  - after(), older()
  - and(), or(), thresh()

Miniscript

- Examples:
  - and(pk(A), pk(B))
  - thresh(2, pk(A), pk(B), older(144))
  - and(pk(user),or(99@pk(service),older(144)))

Miniscript

- Once we have a Miniscript *Policy* we can use a compiler to get a Bitcoin script
  - Small search space => brute force for the best solution
  - Some policies have multiple equivalent scripts!!
  - Make backups a nightmare

Descriptors

- We need an intermediate representation
  - Still (kinda) human readable
  - Always maps 1:1 with Bitcoin scripts
  - The syntax looks similar but it’s more complex
  - Bonus: encode the type of script

Descriptors

- Examples:
  - sh(wsh(and_v(v:pk(A),pk(B))))
  - sh(thresh(2,pk(A),s:pk(B),sdv:older(144)))
  - wsh(and_v(or_c(pk(service),v:older(144)),pk(user)))

Putting It Together

- Write a policy
- Compile to descriptor
- **Backup the descriptor!!**
- Create a wallet instance
  - Get address
  - Sync
  - Spend

BIP 157/158

- AKA Compact Filters
- AKA Neutrino
- For every block produce a smaller index called *block filter*
- Light clients fetch all the filters
- Match against the filters
- Only download the necessary full blocks

BIP 157/158

- BIP 157 => Network messages to exchange filters
- BIP 158 => Filter type 0x00
  - Index by output addresses and spent utxos

BIP 157/158

- BIP 157 sync similar to syncing headers
  - Additional `getcfcheckpt` message
  - Easy to detect conflicts between peers
  - Allows to download the filters in parallel

BIP 157/158

- Better than BIP 37 (Bloom Filters):
  - More private
  - Stateless
    - Filters can be cached statically in a CDN-like fashion
    - Even via DNS https://bitcoinheaders.net/

BIP 157/158

- Still takes a decent amount of bw
- There are no filters for the mempool
  - If you want to see an unconfirmed tx you need to download the full mempool

Bonus: TA


BTC/USD 4 hour Technical Analysis by afilini
Maximum Level for extended wave 20.3k to 20.6k
21D MA
This blue line is the 21D MA which is the most important indicator we need to keep an eye on.