Miniscript

Safe and Standard Wallets

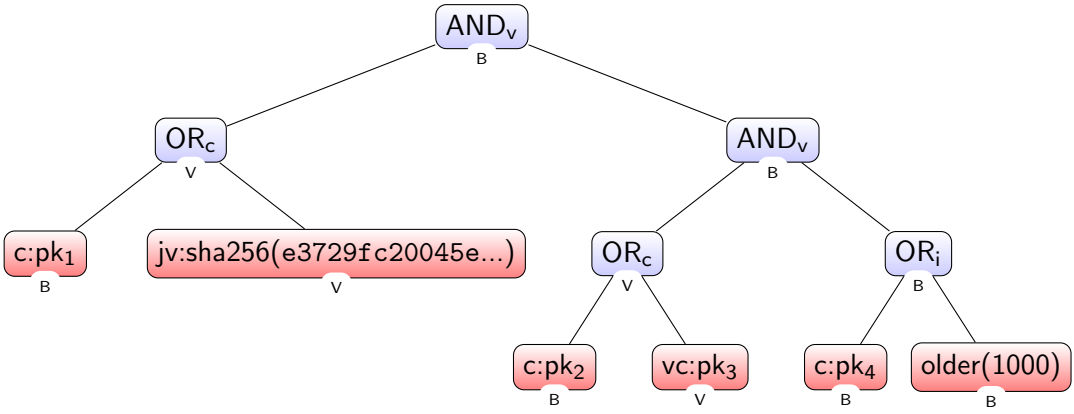
-

- 1Lsbc1NQ6jgLovgwzDmkobV8HocTVghimp
- 3FdNzkJmdX7bWDYKvAZnv1VKQ4PvPobCib
- bc1q2s2kgmf244jmx3exkst94lssum520grsjewxkk

-

```
pk1 CHECKSIG
   NOTIF SIZE 32 EQUALVERIFY SHA256 e3729fc20045e8b5 EQUALVERIFY ENDIF
   pk2 CHECKSIG NOTIF pk3 CHECKSIGVERIFY ENDIF
   IF pk4 CHECKSIG ELSE 1000 CSV ENDIF
```

-


AND$_v$
B
OR$_c$
V
AND$_v$
B
c:pk$_1$
B
jv:sha256(e3729fc20045e...)
V
OR$_c$
V
OR$_i$
B
c:pk$_2$
B
vc:pk$_3$
V
c:pk$_4$
B
older(1000)
B

-

Key Management

- What is the script?
- Is it secure?
- What keys do I need?
- What will it cost?

Interoperability

- Can I use a new device?
- Does my policy fit into the big picture?
- Can I securely multisign/coinjoin with heterogeneous setups?

Thank You

Andrew Poelstra
miniscript@wpsoftware.net

https://bitcoin.sipa.be/miniscript

https://github.com/apoelstra/rust-miniscript