M I N I S C R I P T

Custody. Computable. Composeable.

Andrew Poelstra
Director of Research, Blockstream

November 6, 2021

Issues with Bitcoin Script

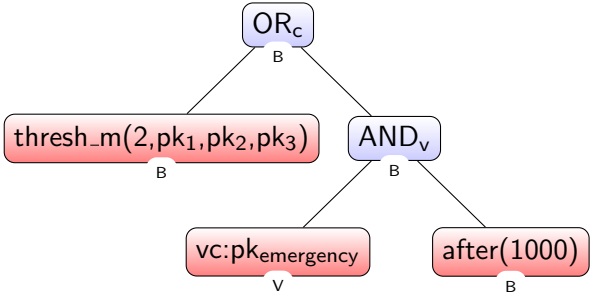
- Difficult to argue correctness (or other properties)
- Difficult to argue security (or malleability freeness)
- Difficult to estimate satisfaction cost
- Difficult to determine which signatures are needed
- Difficult to assemble a witness, even given signatures

Issues with Bitcoin Script

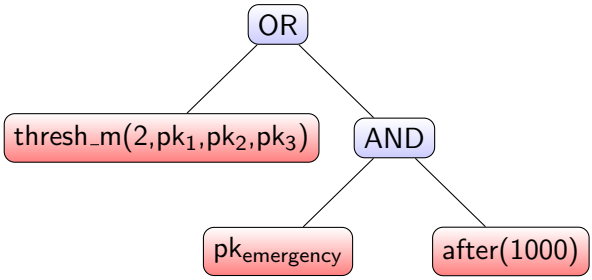
- Not interoperable between wallet implementations
- Not composeable within wallets

- Idea: create script templates for signature checks, hash-locks and time-locks
- Idea: create composable script templates for AND, OR and thresholds

```
2 pk1 pk2 pk3 3 CHECKMULTISIG
IFDUP NOTIF
    pkemergency CHECKSIGVERIFY
    1000 CSV
ENDIF
```



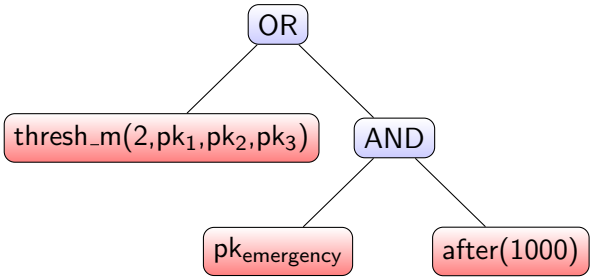
```
2 pk1 pk2 pk3 3 CHECKMULTISIG
IFDUP NOTIF
    pkemergency CHECKSIGVERIFY
    1000 CSV
ENDIF
```



Script and Miniscript

- In a technical sense, Miniscript is a subset of Script.
- In a non-technical sense, Miniscript works in a different paradigm than Script
- Miniscript describes conditions to satisfy, not instructions to execute

[some totally different language]



Future Work

- Further Integration with PSBT
- Library development (`rust-bitcoin`, `bdk`)
- Taproot support!
- Connections to other languages (Script+`CTV`, Simplicity)

Thank You

Andrew Poelstra
miniscript@wpsoftware.net

https://bitcoin.sipa.be/miniscript