Descriptor Wallet: library and command-line

Dr Maxim Orlovsky,
Pandora Core AG

Call agenda

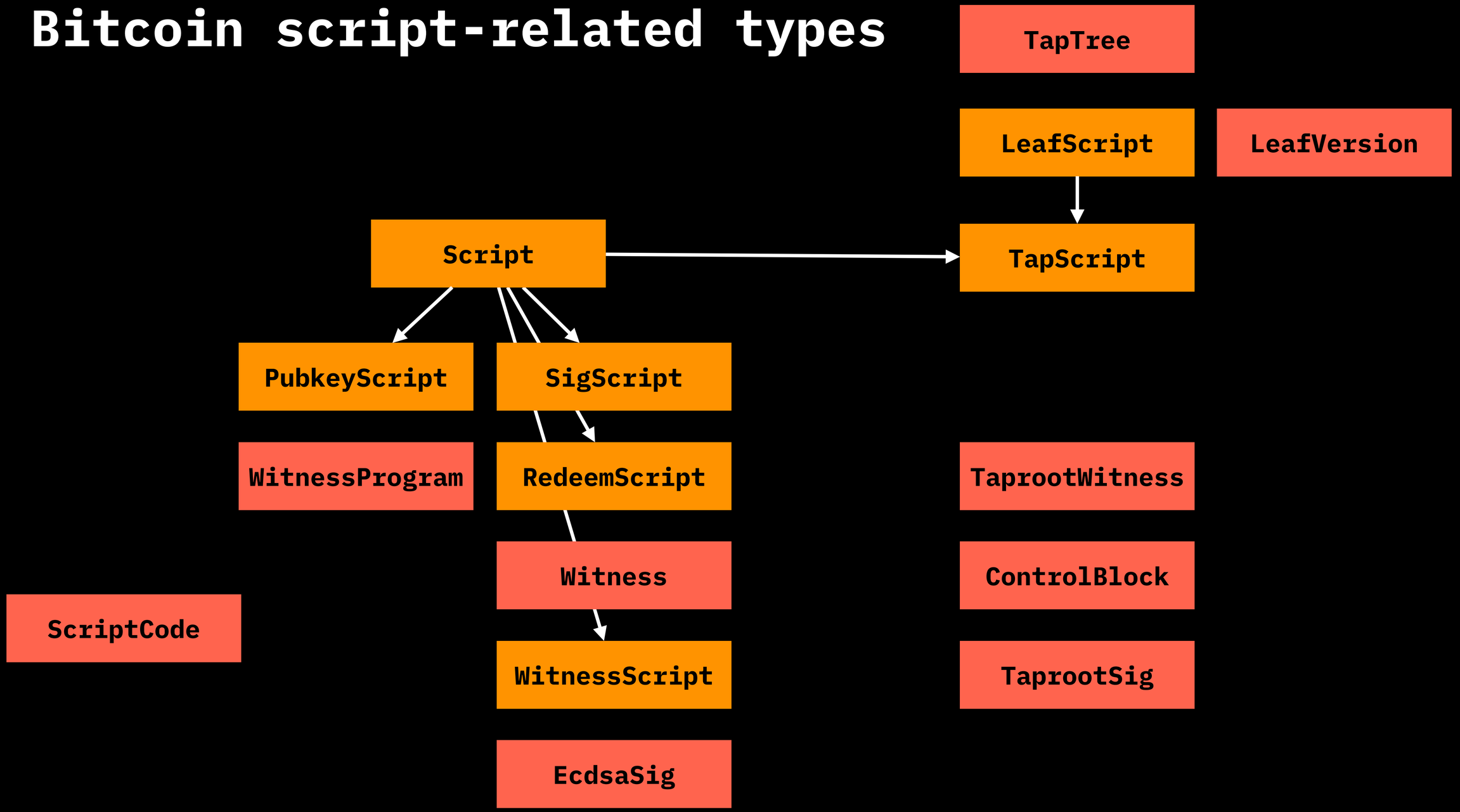
- Descriptor wallet intro
- Descriptor wallet demo
- Wallet challenges related to RGB & single-use-seals
- P2C & S2C commitment discussion

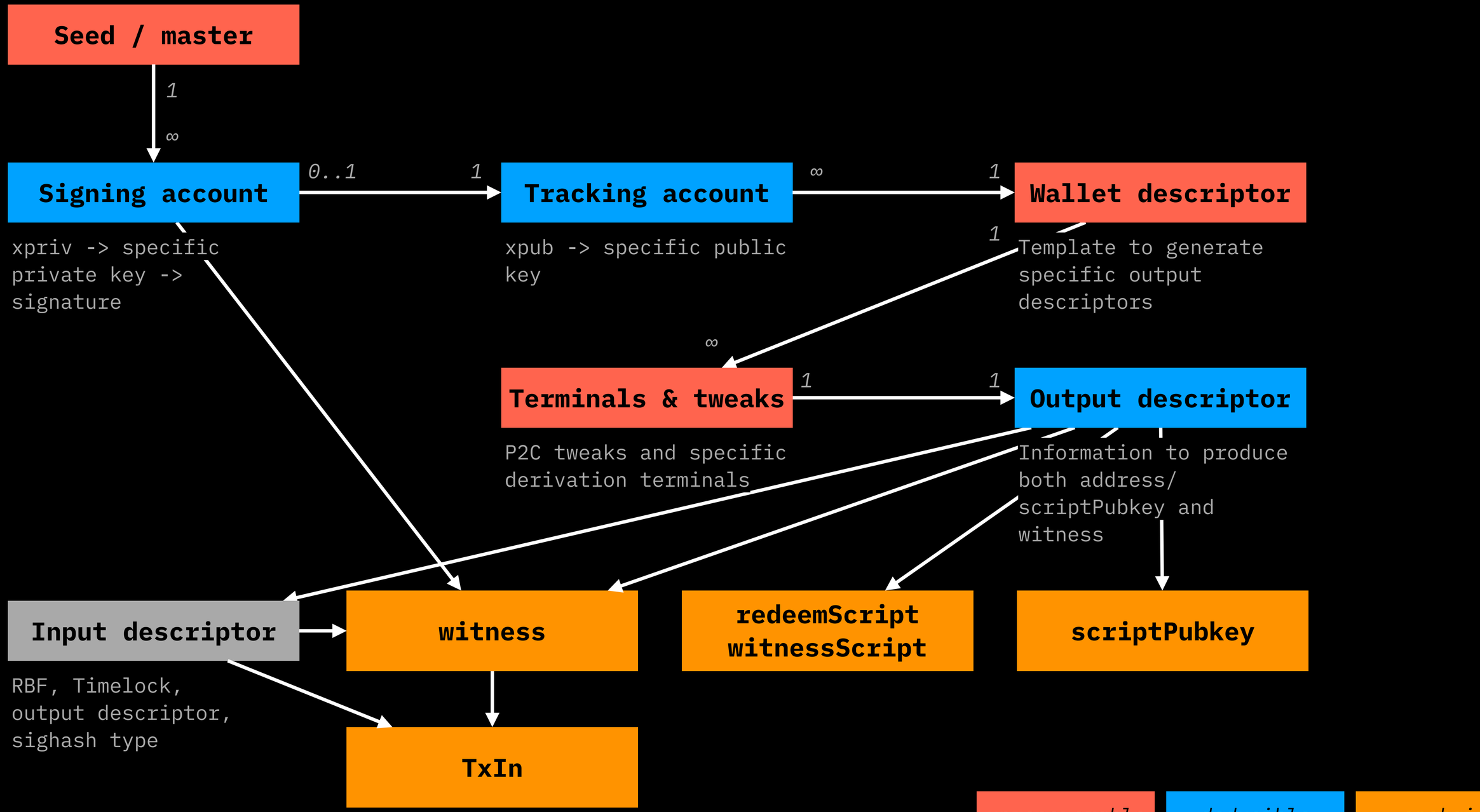
Descriptor wallet

- Separating cold and hot parts
- Allowing P2C / S2C commitments & single-use-seals
- Foundation for LNP Node, RGB Node, MyCitadel Wallet
- Pro command-line tool to do arbitrary-complex magic with bitcoin

	Descriptor Wallet	BitcoinDevKit	Green dev kit (GDK)	Libwally	All other wallet libraries
Full hot/cold wallet isolation	✅	🚫	🚫	🚫	🚫
Output descriptors	✅	✅	🚫	🚫	🚫
Input descriptors	✅	🚫	🚫	🚫	🚫
Miniscript	✅	✅	🚫	🚫	🚫
Taproot base	✅	✅	🚫	🚫	🚫
Taproot MuSig2	🚫	🚫	🚫	🚫	🚫
TapScript	✅	✅	🚫	🚫	🚫
P2C tweaks	✅	🚫	🚫	🚫	🚫
Custom sighashes	✅	🚫	🚫	🚫	🚫
Lightning compatibility	✅	🚫	🚫	🚫	🚫

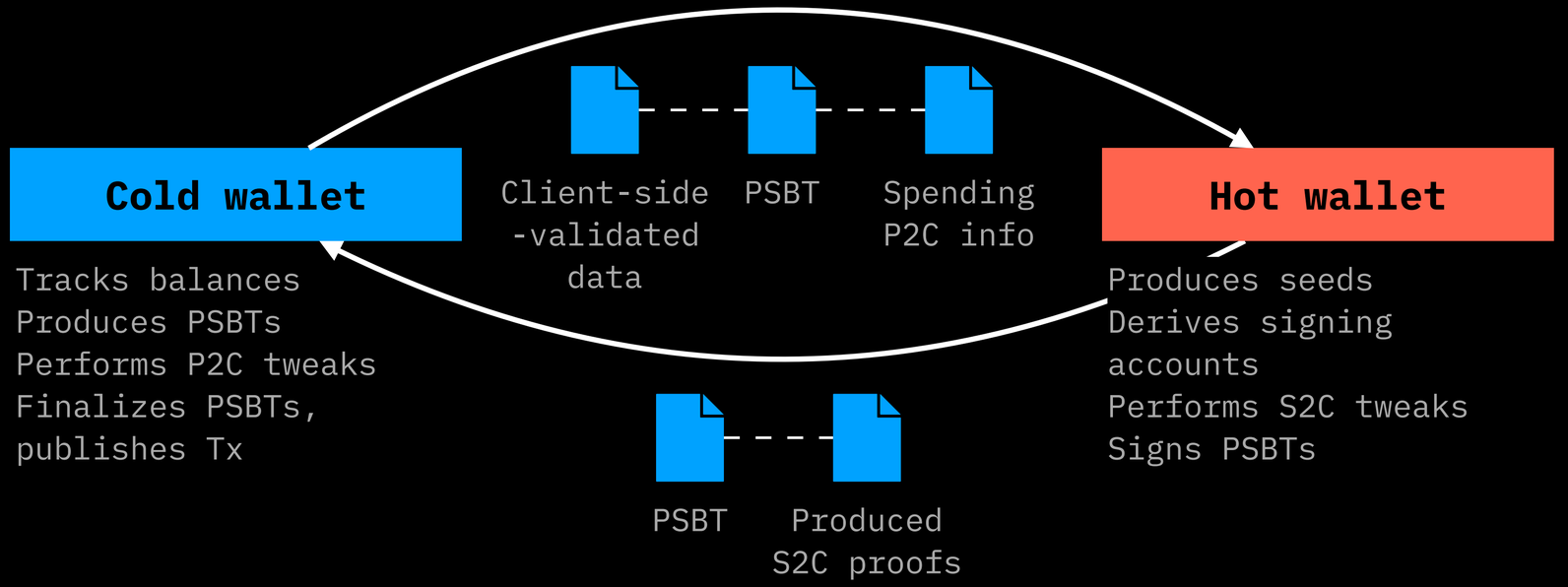
Bitcoin script-related types




Seed / master
1
∞
Signing account
0..1
1
Tracking account
∞
1
Wallet descriptor
xpriv -> specific private key -> signature
xpub -> specific public key
1
Template to generate specific output descriptors
∞
Terminals & tweaks
1
1
Output descriptor
P2C tweaks and specific derivation terminals
Information to produce both address/ scriptPubkey and witness
Input descriptor
witness
redeemScript witnessScript
scriptPubkey
RBF, Timelock, output descriptor, sighash type
TxIn
unrecoverable
deducible
onchain

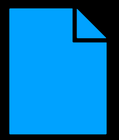
Demo

Cold-hot wallet distinction



Contact identities

Tracking accounts



Wallet descriptor

Tweak Information

Client-side-validation state commitments

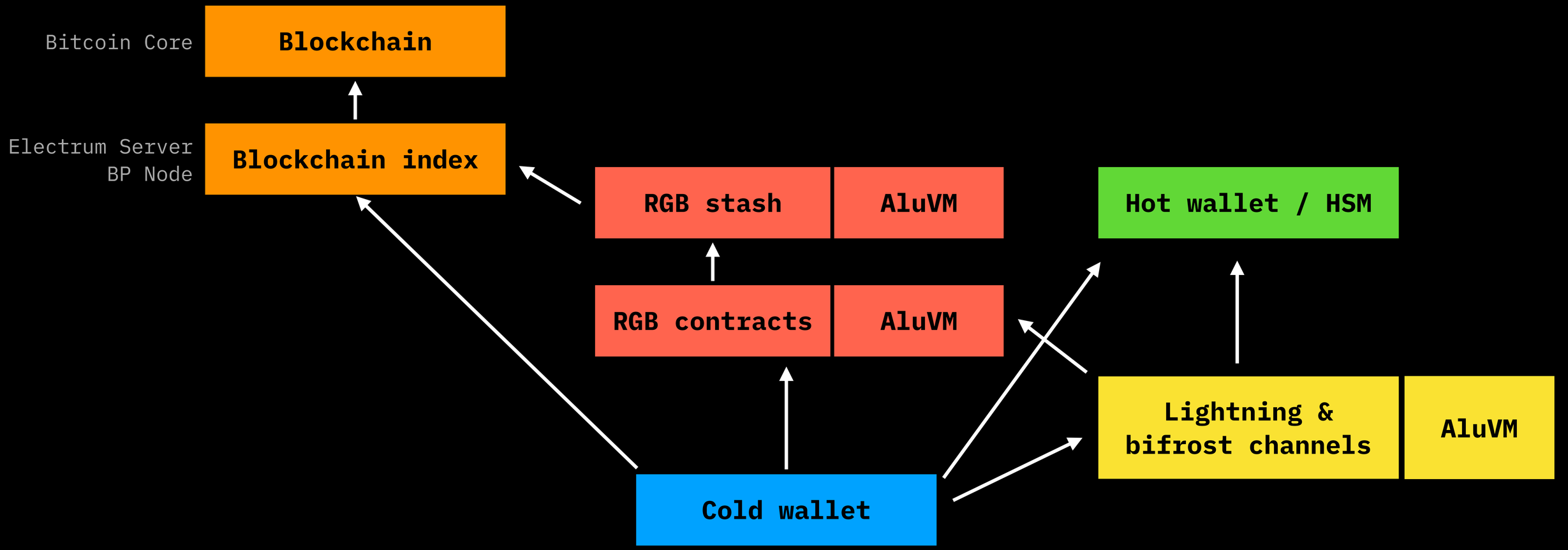
Signing accounts

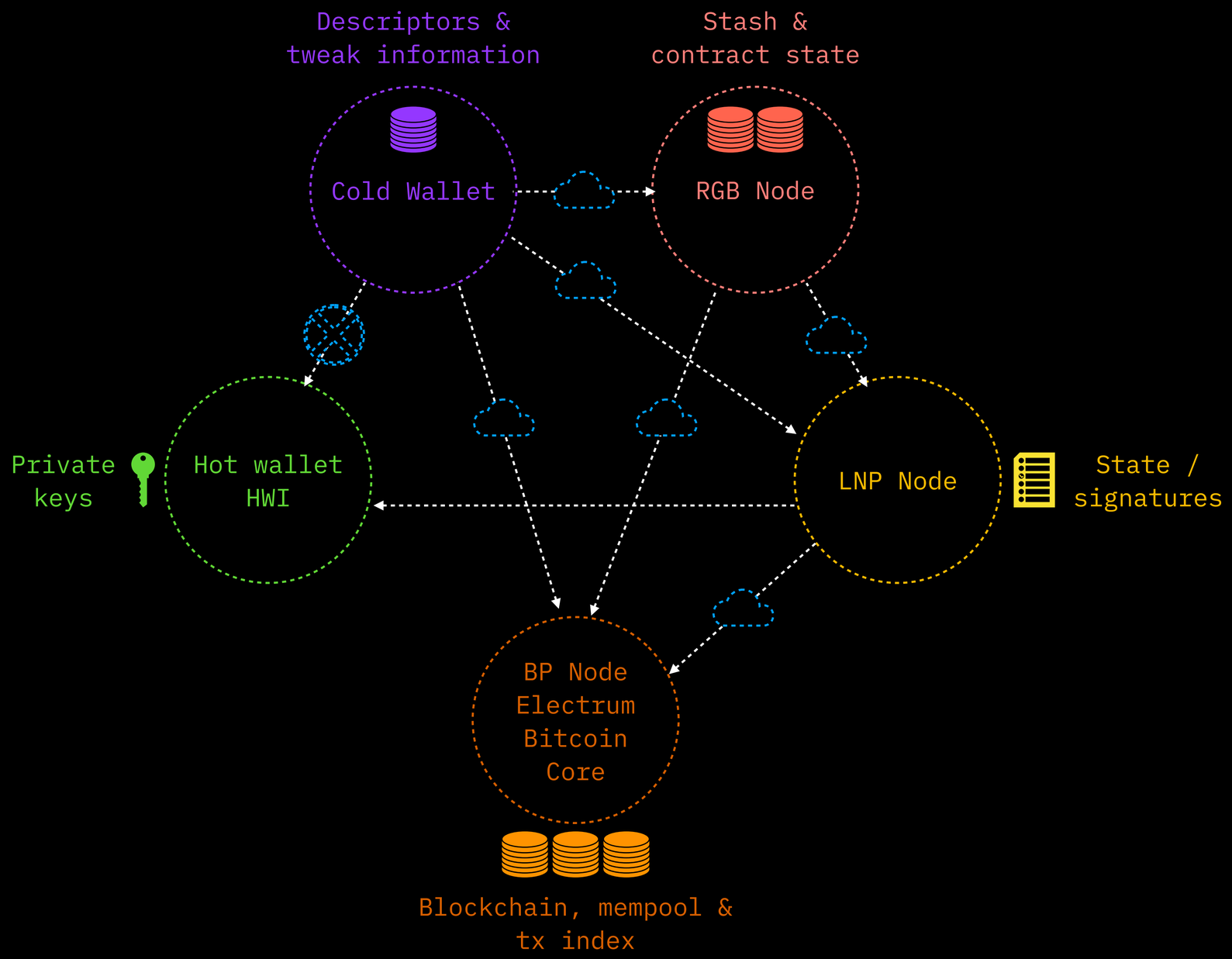
Wallet data structures

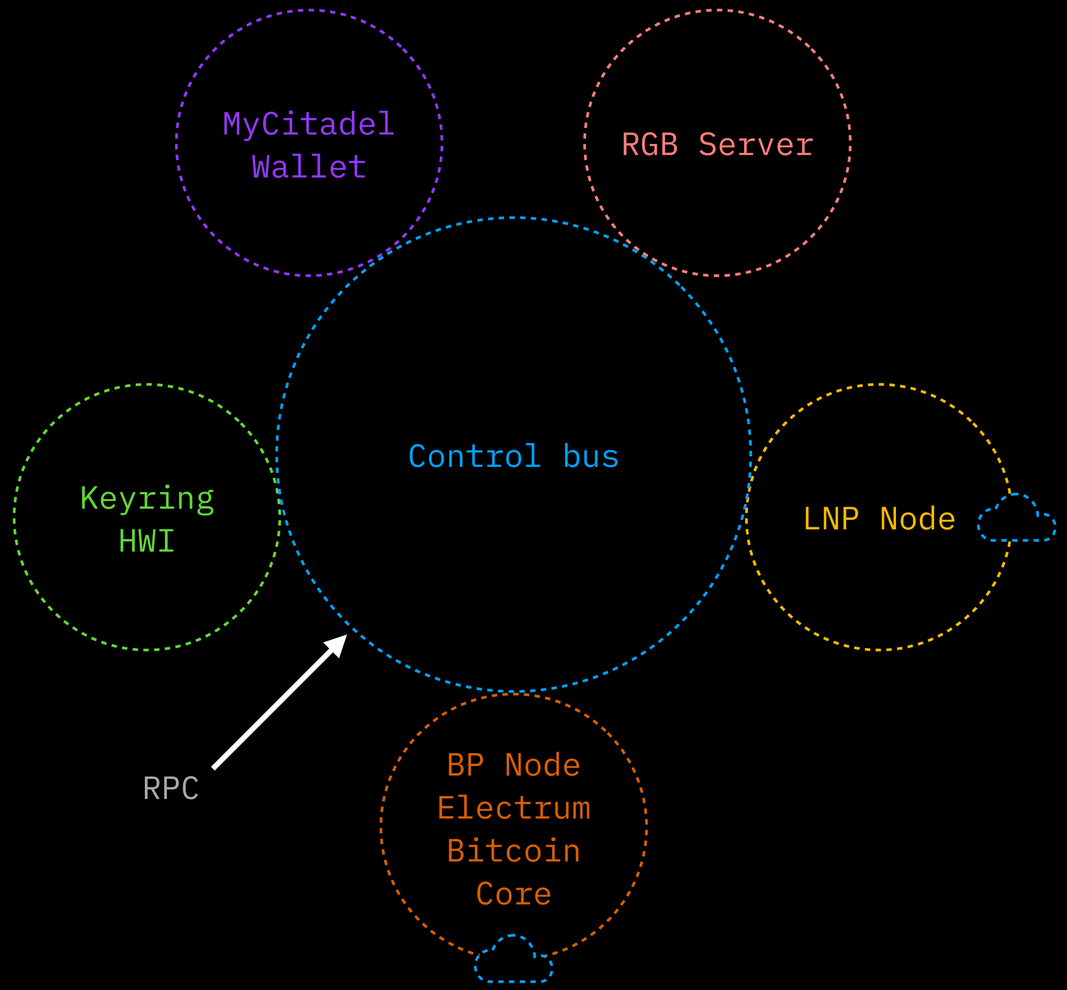
- Seed:
  mnemonic (12..24 words)
- Signing account:
  m=[f1493701]/44’/0’=[xpriv…]
- Tracking account (TA):
  m=[f1493701]/44’/0’=[xpub…]//**
- Wallet descriptor:
  tr(musig(TA1, TA2), {
  and_v(older(5),TA1),
  and_v(older(5),agg(TA1, TA1)
  })
- Terminals & tweaks:
  1/1665~[key_fingerprint]:tweak_hash
- Output descriptor:
  wsh(
  sortedmulti([fp1]~hash, [fp2])
)@1/1665
- Input descriptor:
  wsh(
  sortedmulti([fp1]~hash, [fp2])
)@1/1665@rbf#SINGLE

Input descriptor example

- txid:vout /1/167 [deadbeef]+hash rbf SIGHASH_ALL


Bitcoin Core
Blockchain
Electrum Server
BP Node
Blockchain index
RGB stash
AluVM
RGB contracts
AluVM
Hot wallet / HSM
Lightning &
bifrost channels
AluVM
Cold wallet


Descriptors &
tweak information
Stash &
contract state
Cold Wallet
RGB Node
Private
keys
Hot wallet
HWI
LNP Node
State /
signatures
BP Node
Electrum
Bitcoin
Core
Blockchain, mempool &
tx index


MyCitadel
Wallet
RGB Server
Control bus
Keyring
HWI
LNP Node
RPC
BP Node
Electrum
Bitcoin
Core