taproot

peter opara
15.12.2021

Bitcoin Ljubljana

- schnorr signatures
- MAST (merkelized abstract syntax tree)
- taproot

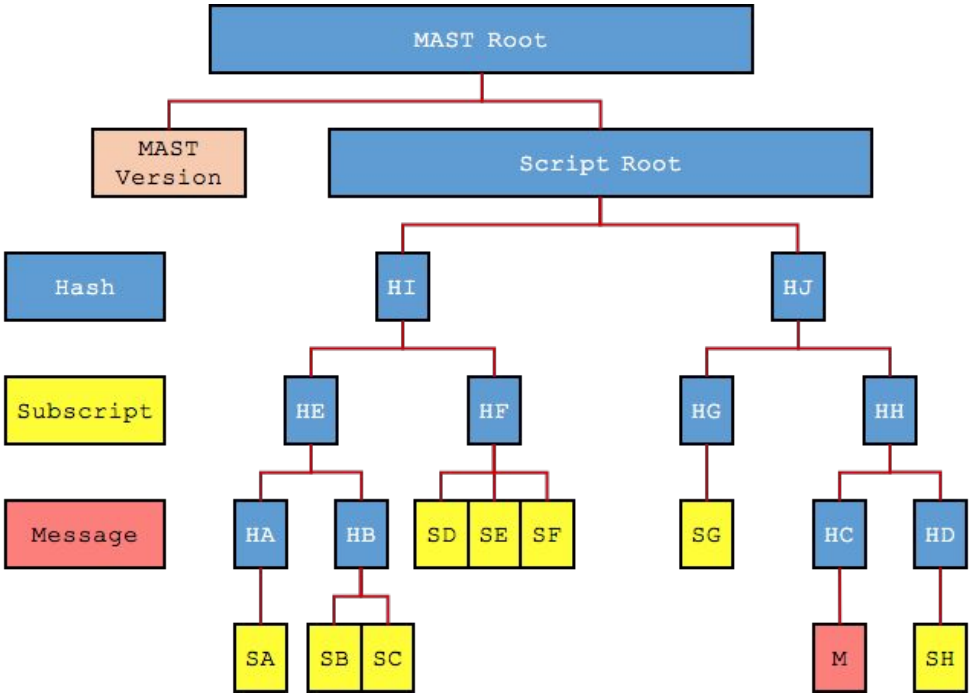
schnorr signatures

privA + privB = privC

pubA + pubB = pubC

pubC + m = pubD

MAST (merkelized abstract syntax tree)



taproot

C + hash(C||m)G = P

A + B + hash(C||m)G = P

a + b + hash(C||m) = p

spend by providing sig for P

m = “<timeout> OP_CSV OP_DROP B OP_CHECKSIGVERIFY”

spend by revealing C, m and providing witness that evaluates m to true

Providing signature does not reveal that a script existed.

m is a MAST root. You only provide executing subscript and needed hashes