Bitcoin

EECS 388
16 Feb 2015

Over the past few years…

Bitcoin for security researchers

- Distributed, decentralized consensus
- Security-critical application
- Cryptographic soup
- Open source software
- Actually used: ~$1 billion "market cap"
- Actually used by attackers

History

Cryptocash

Hashing Challenge

- Can you find a string who's SHA256 is:

oooooooooooooooooooooooooooooooooooooooooo

- Can you find a string who's **SHA256** hash starts with:

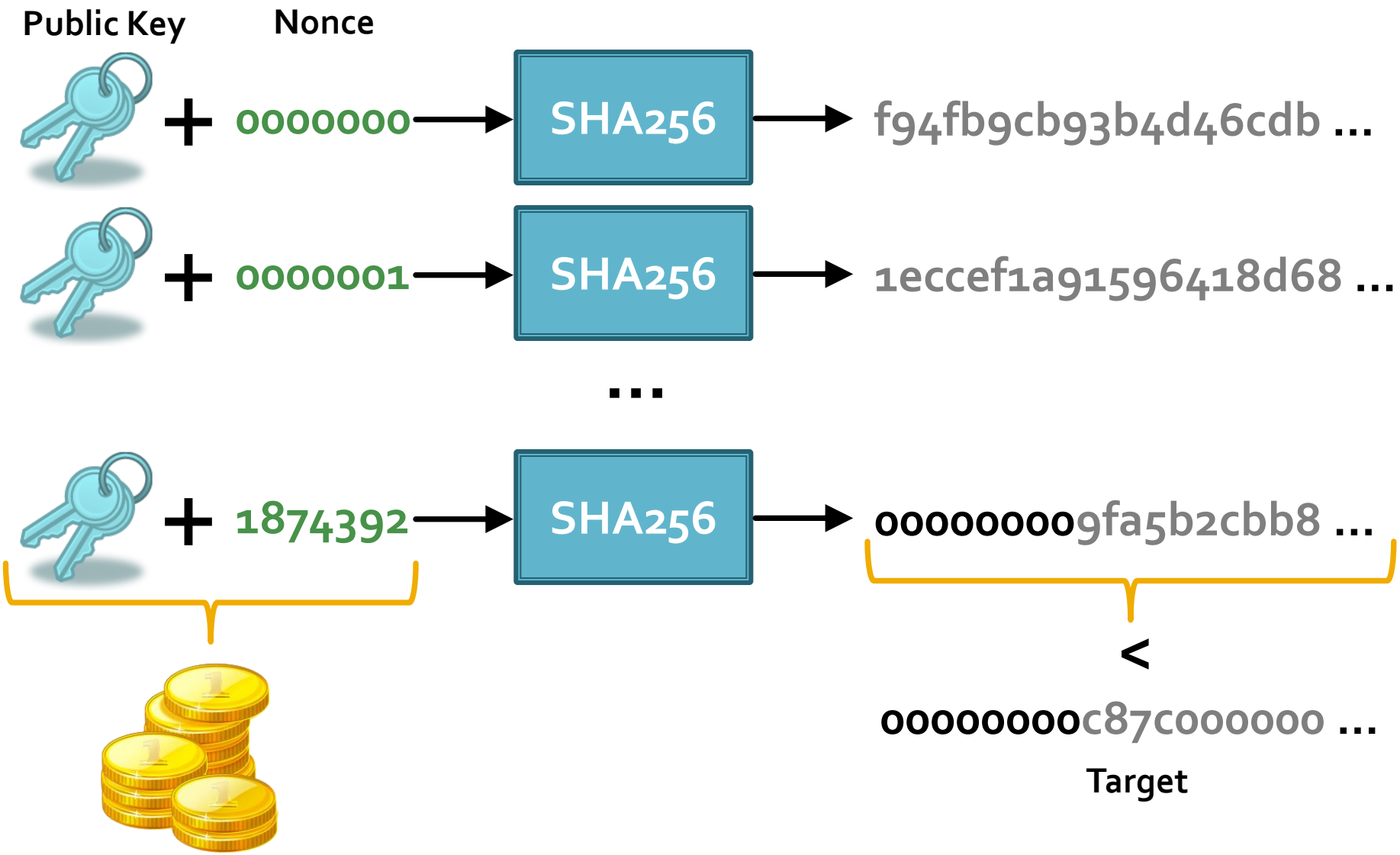
ooooo_____?

SHA256("Michigan Hackerso") =
o21692811f87c04abae44d31691948909 8d48fa13a09 **…**

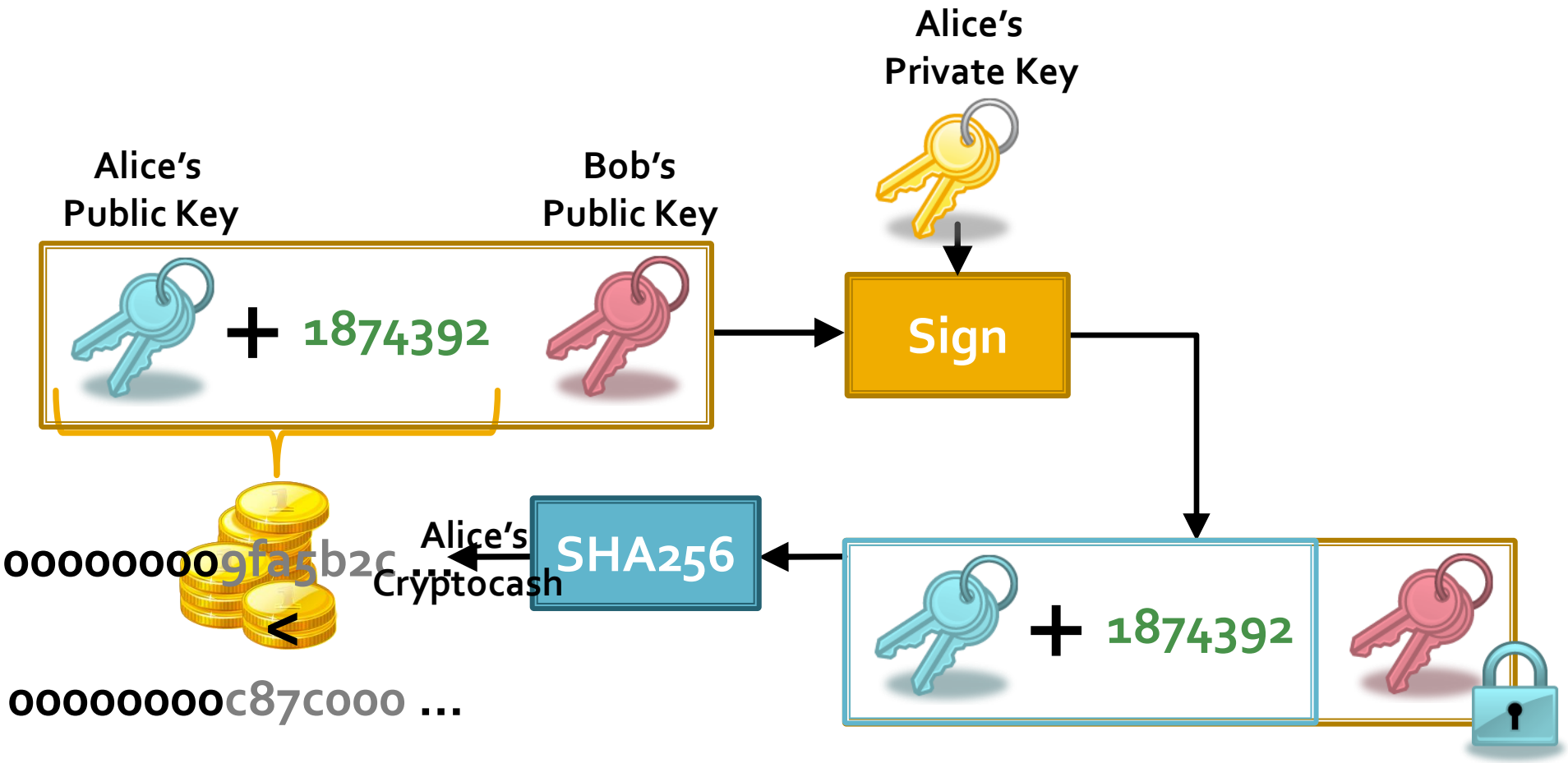
SHA256("Michigan haCkeRS") =
ooa6d212ce548dca3ab9122270f33a752ffd8b0130e **…**

SHA256("micHIGan_HaCkERZ_0031337") =
ooooocd58c06ce48983bd3d31d66c431e01397e7c8e4 **…**

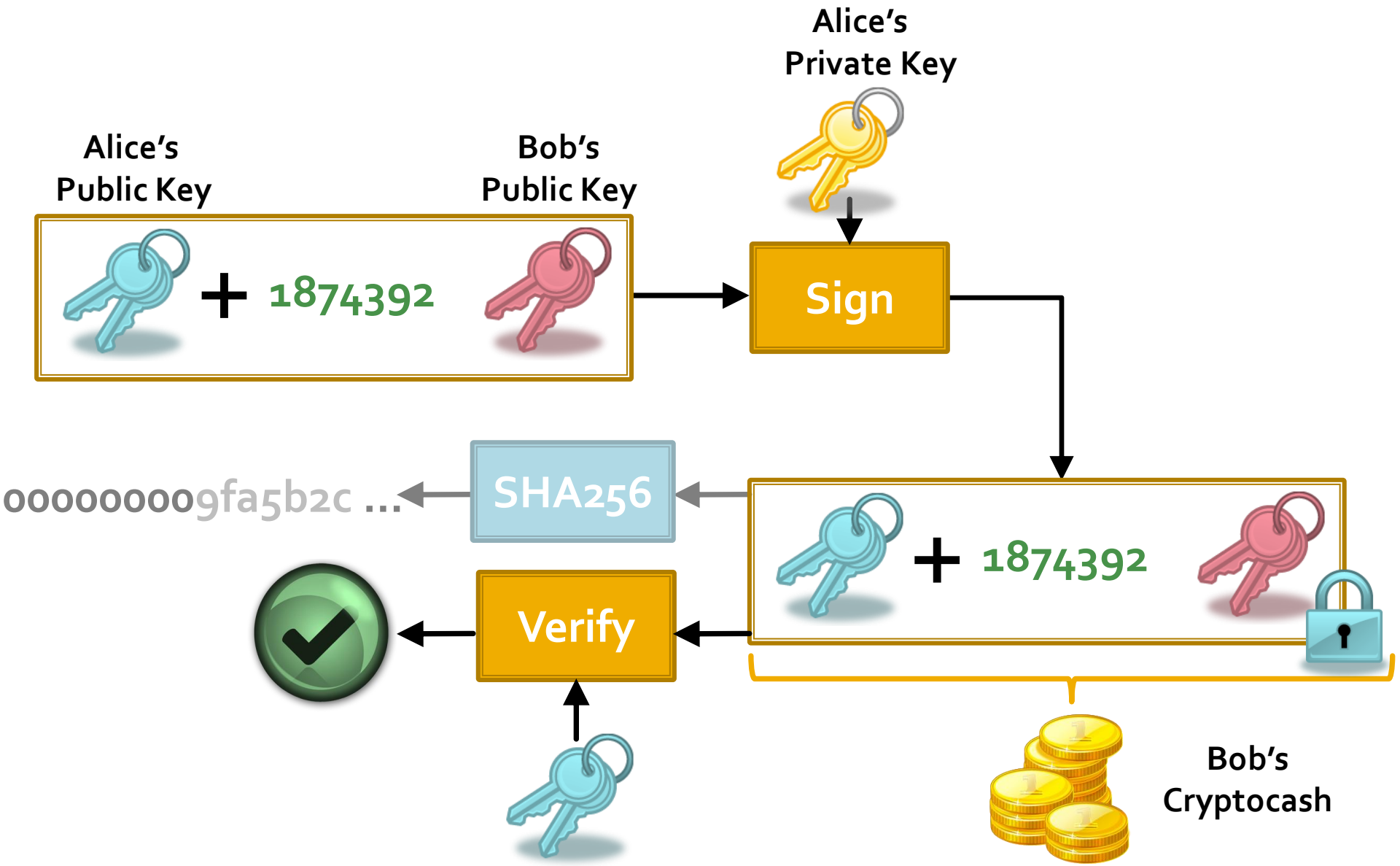
Cryptocash


Public Key
Nonce
+
0000000
SHA256
f94fb9cb93b4d46cdb ...
+
0000001
SHA256
1eccef1a91596418d68 ...
...
+
1874392
SHA256
00000000 9fa5b2cbb8 ...
<
00000000 c87c000000 ...
Target

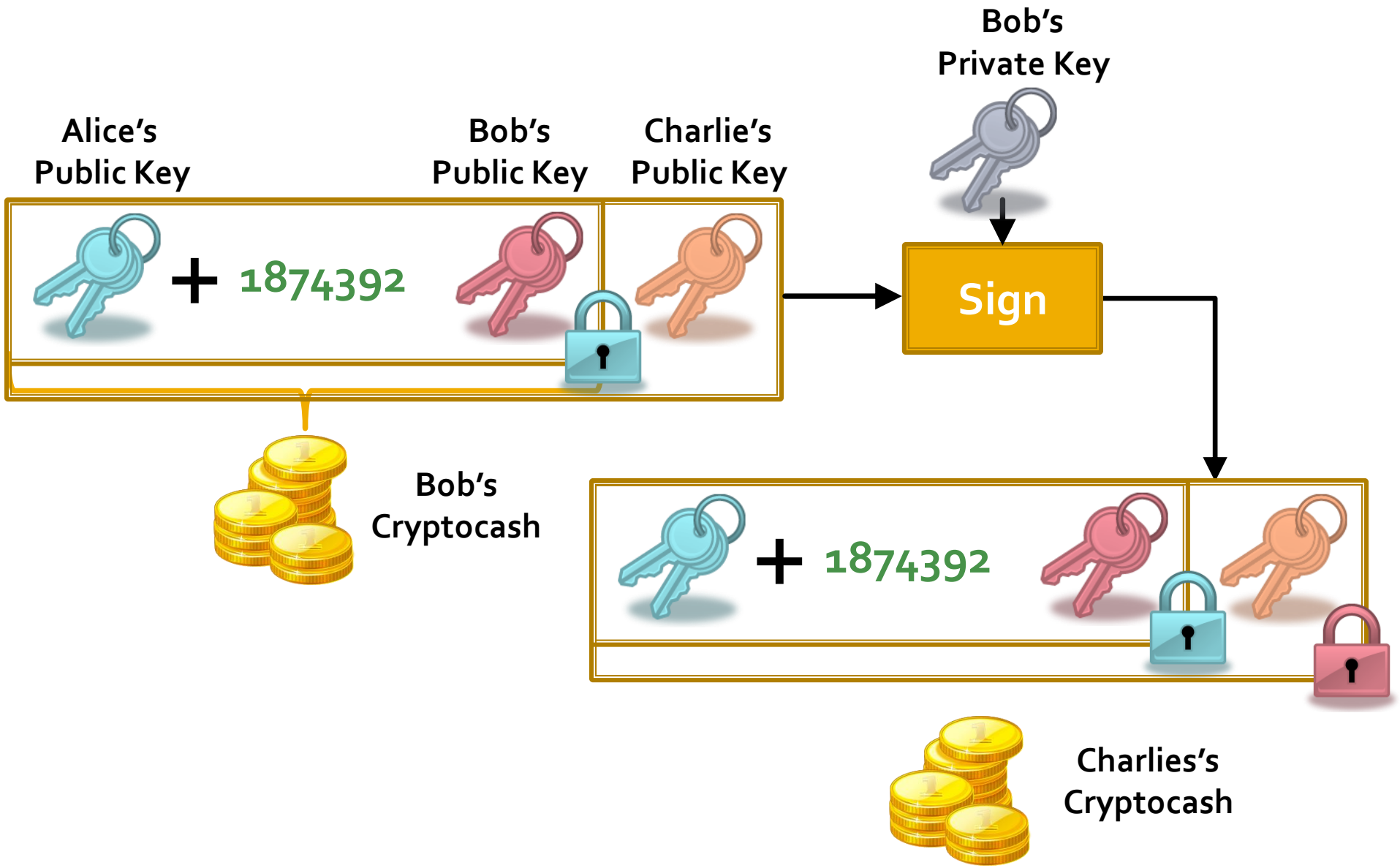
Cryptocash – spending



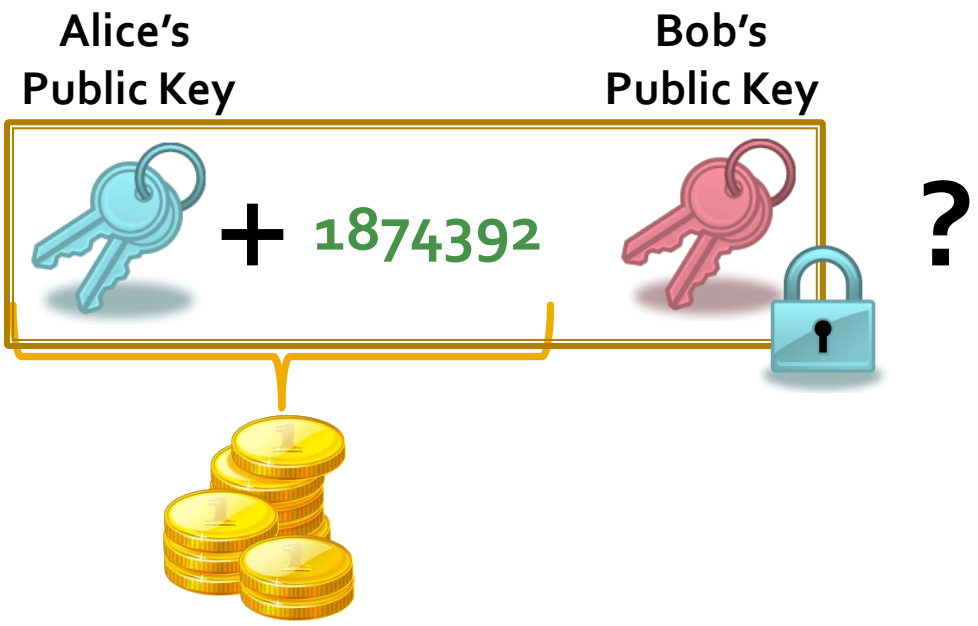
Cryptocash – spending



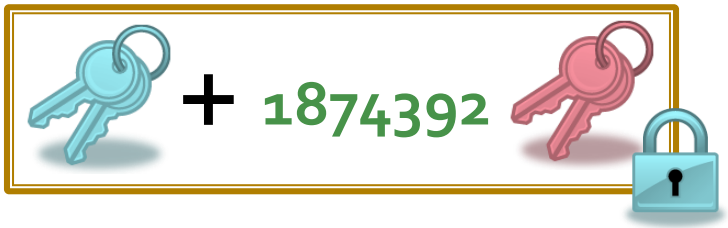
Cryptocash – spending



Cryptocash – double spending



Cryptocash + public ledger

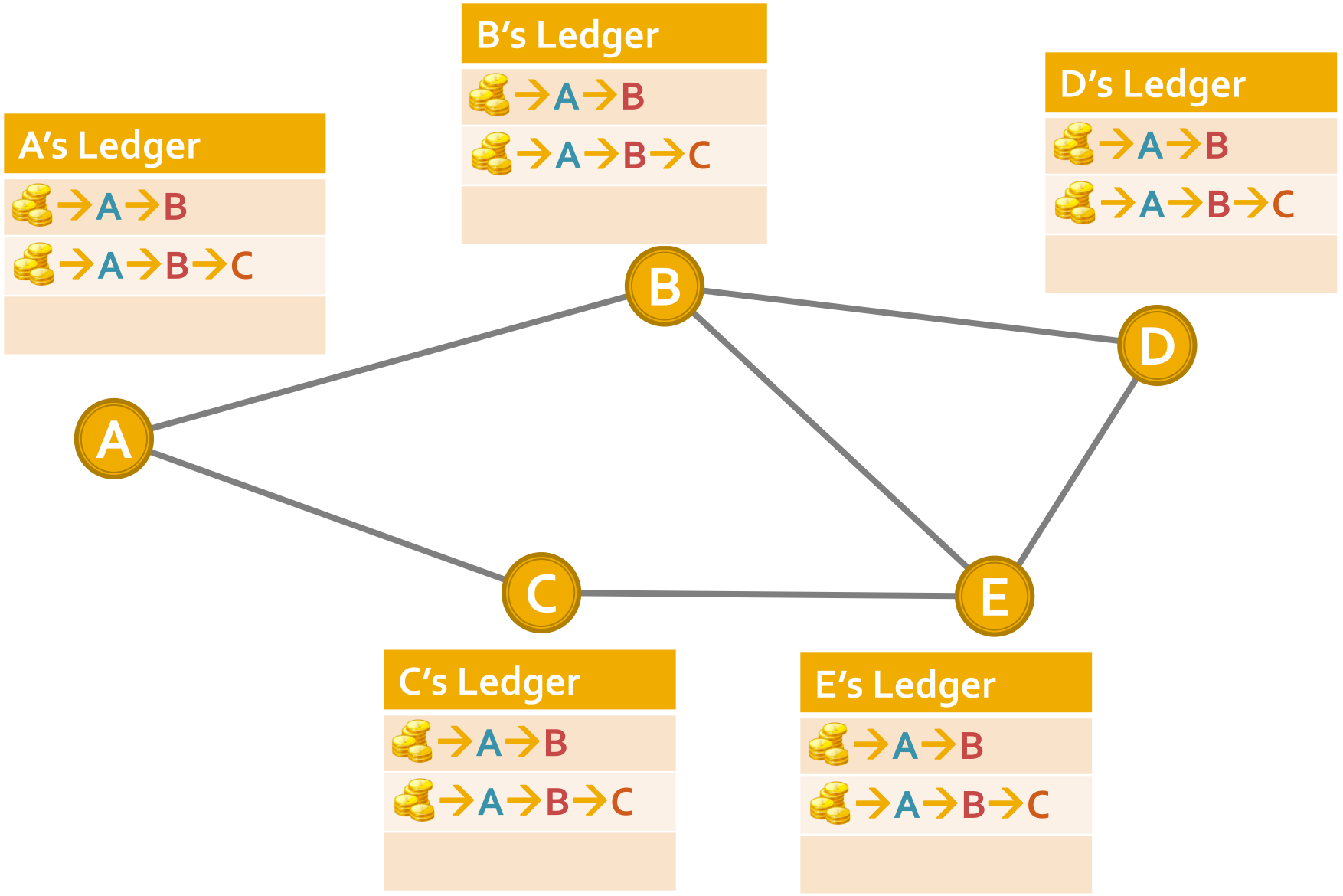


1874392 → Alice → Bob

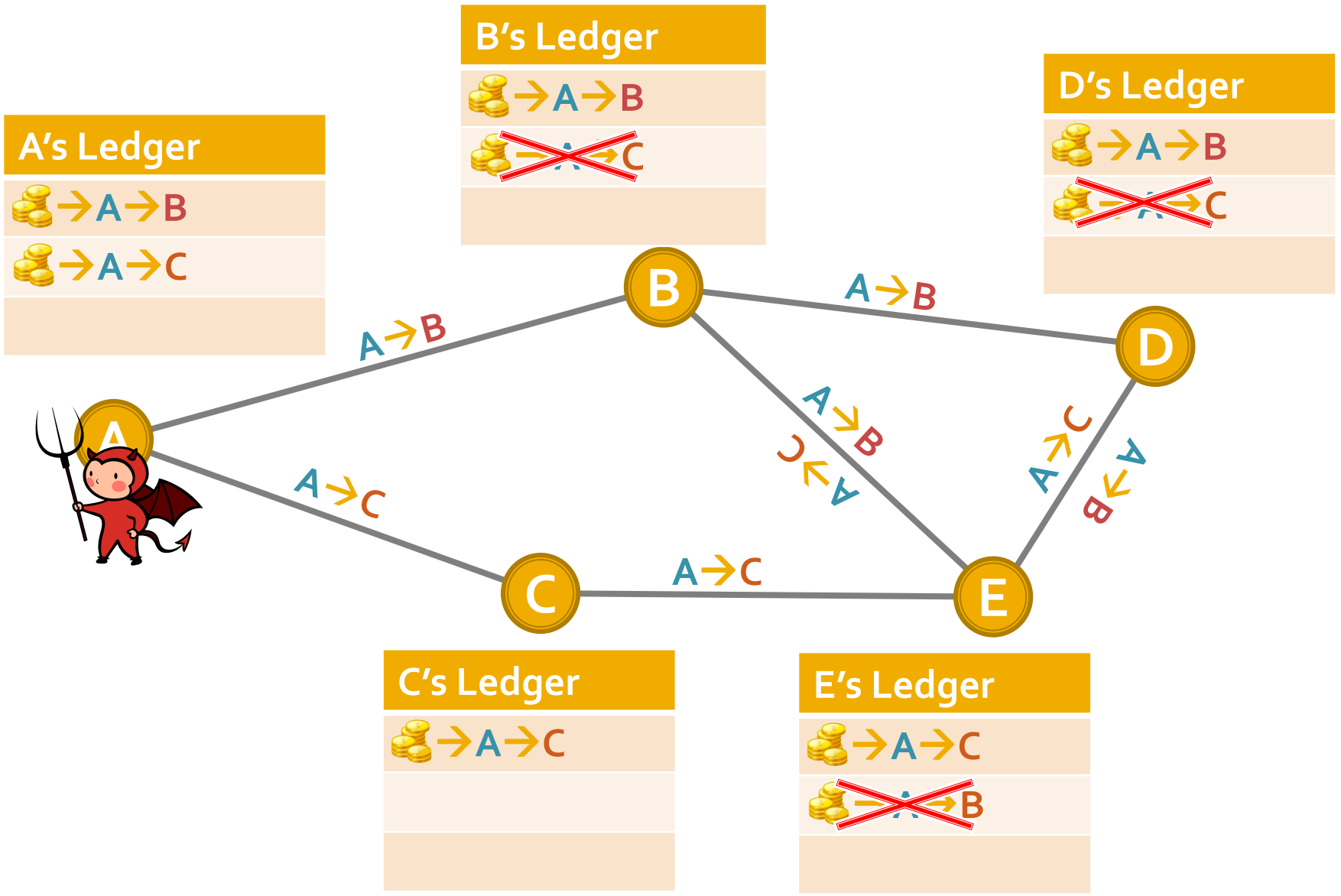
1874392 → Alice → Bob → Charlie

1874392 → Alice → Alice

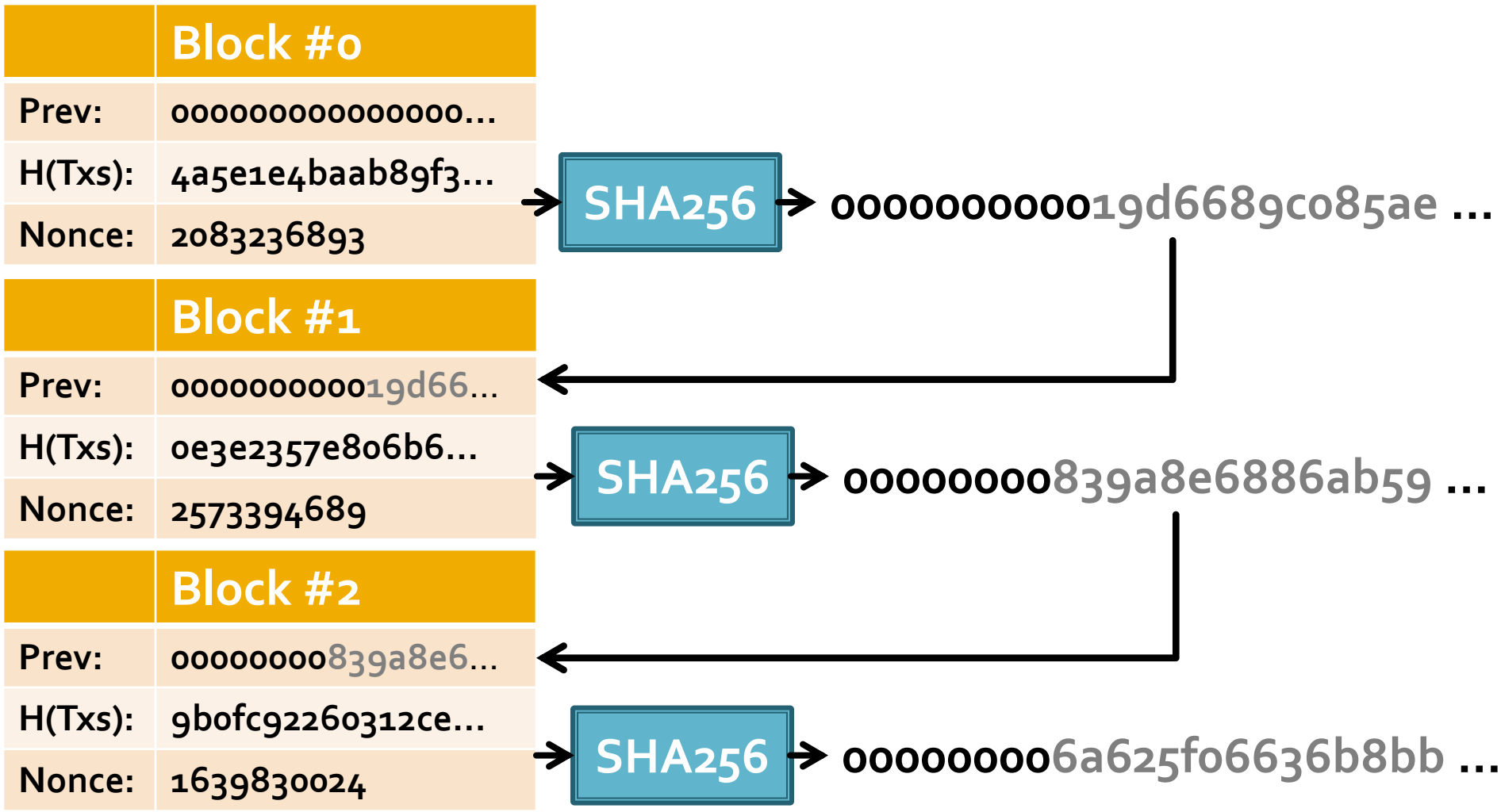
Cryptocash + public ledger(s?)



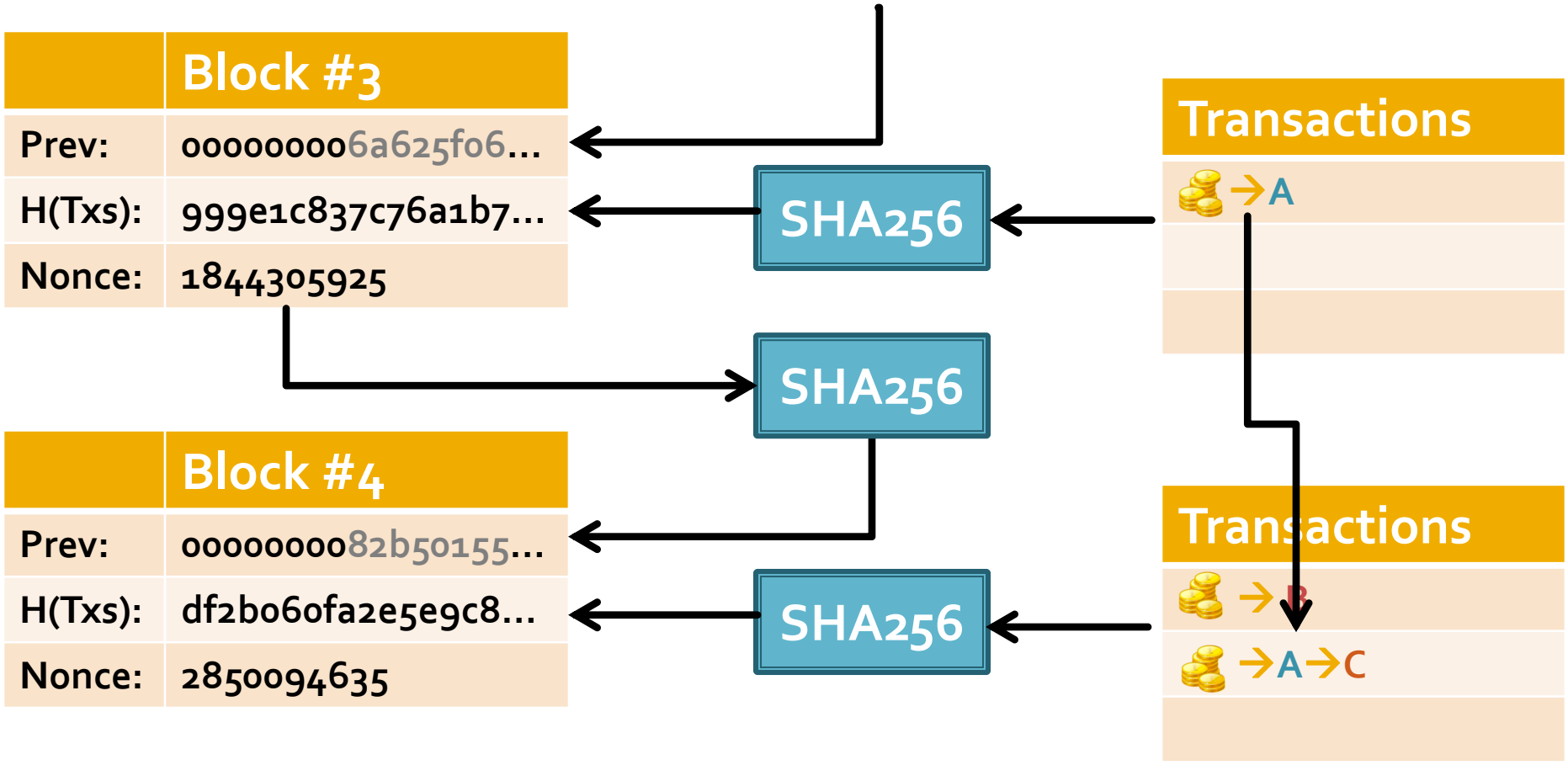
Cryptocash + public ledger(s?)



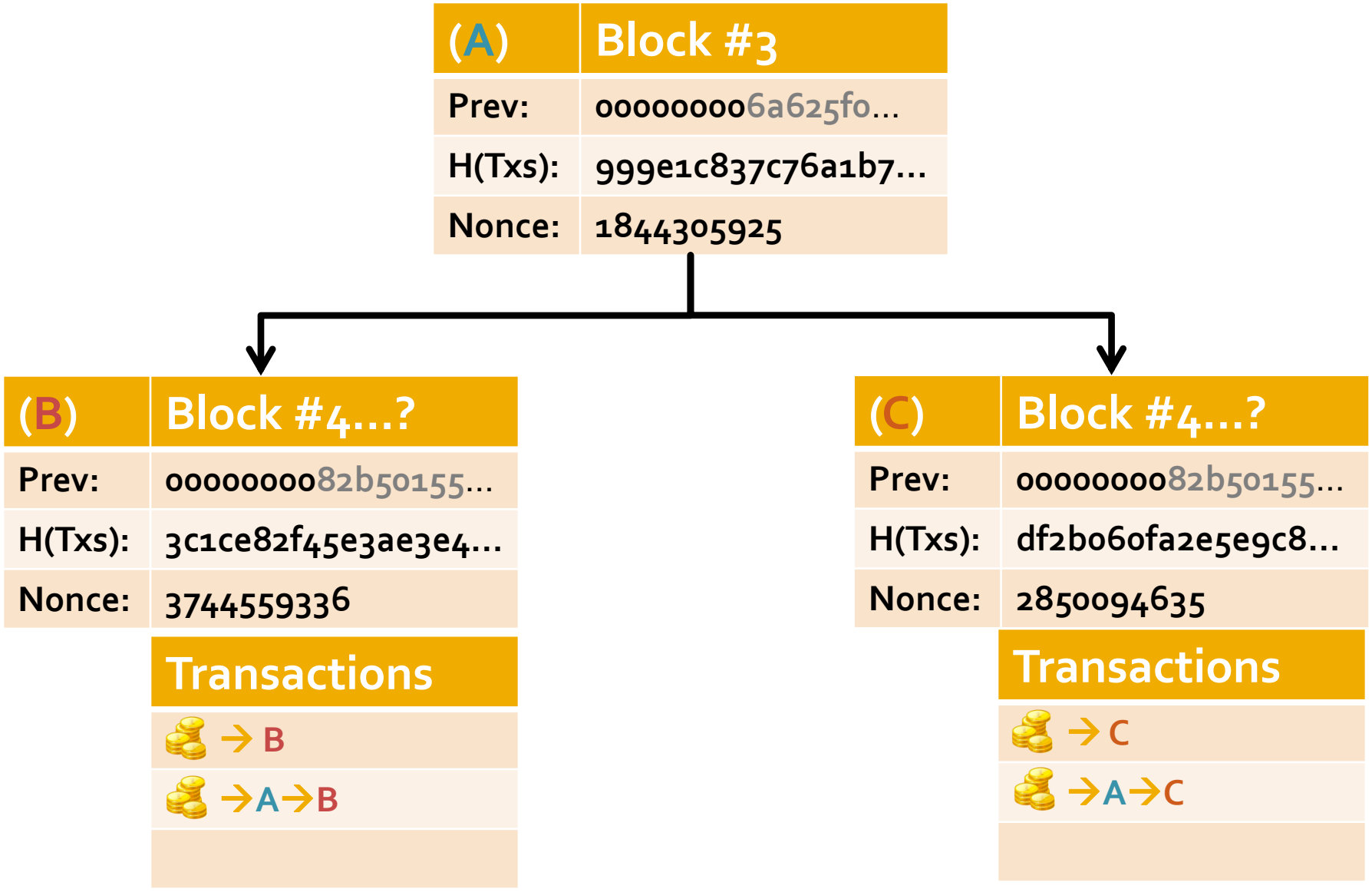
Bitcoin – distributed "consensus"



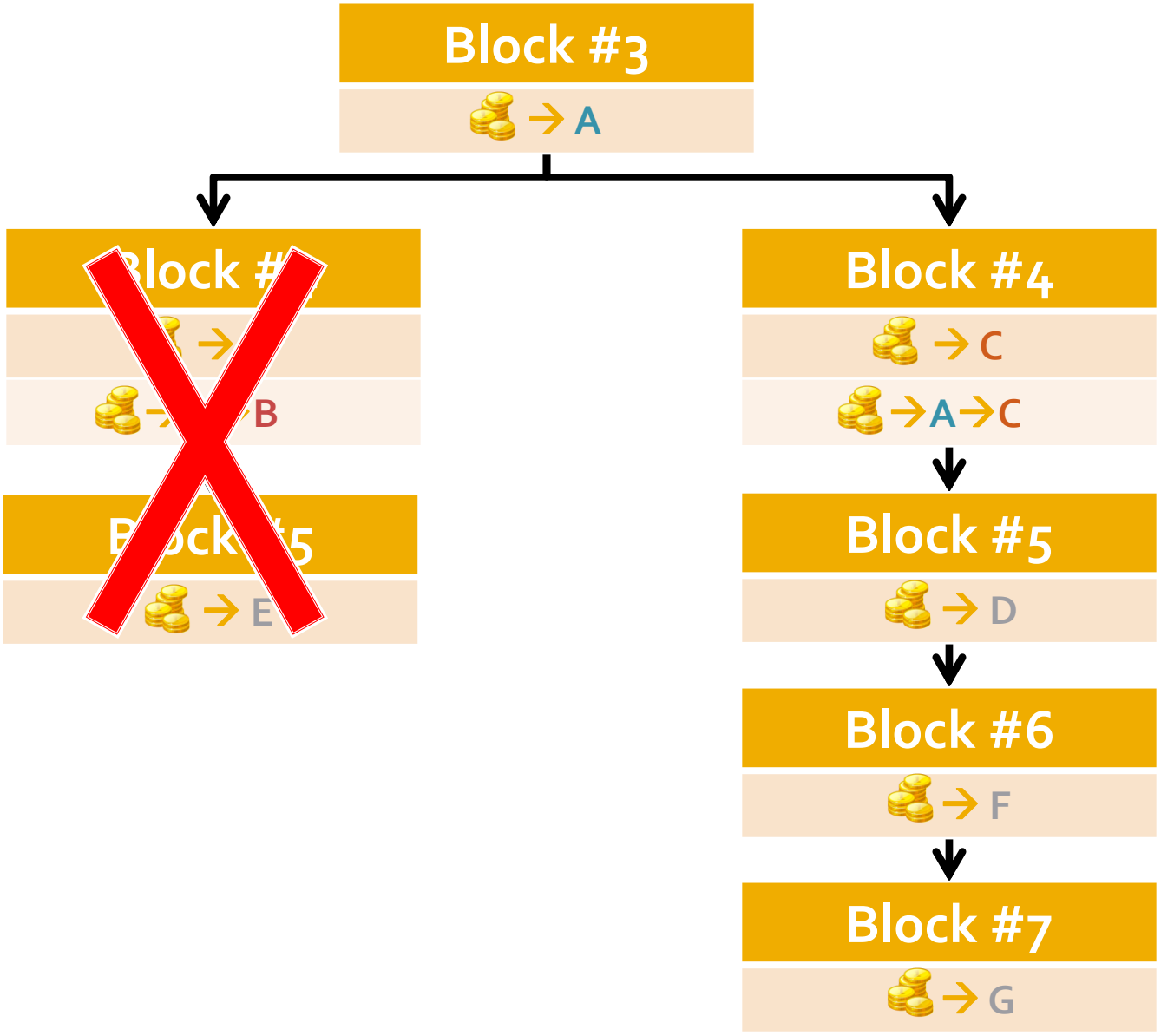
Miner picks transactions



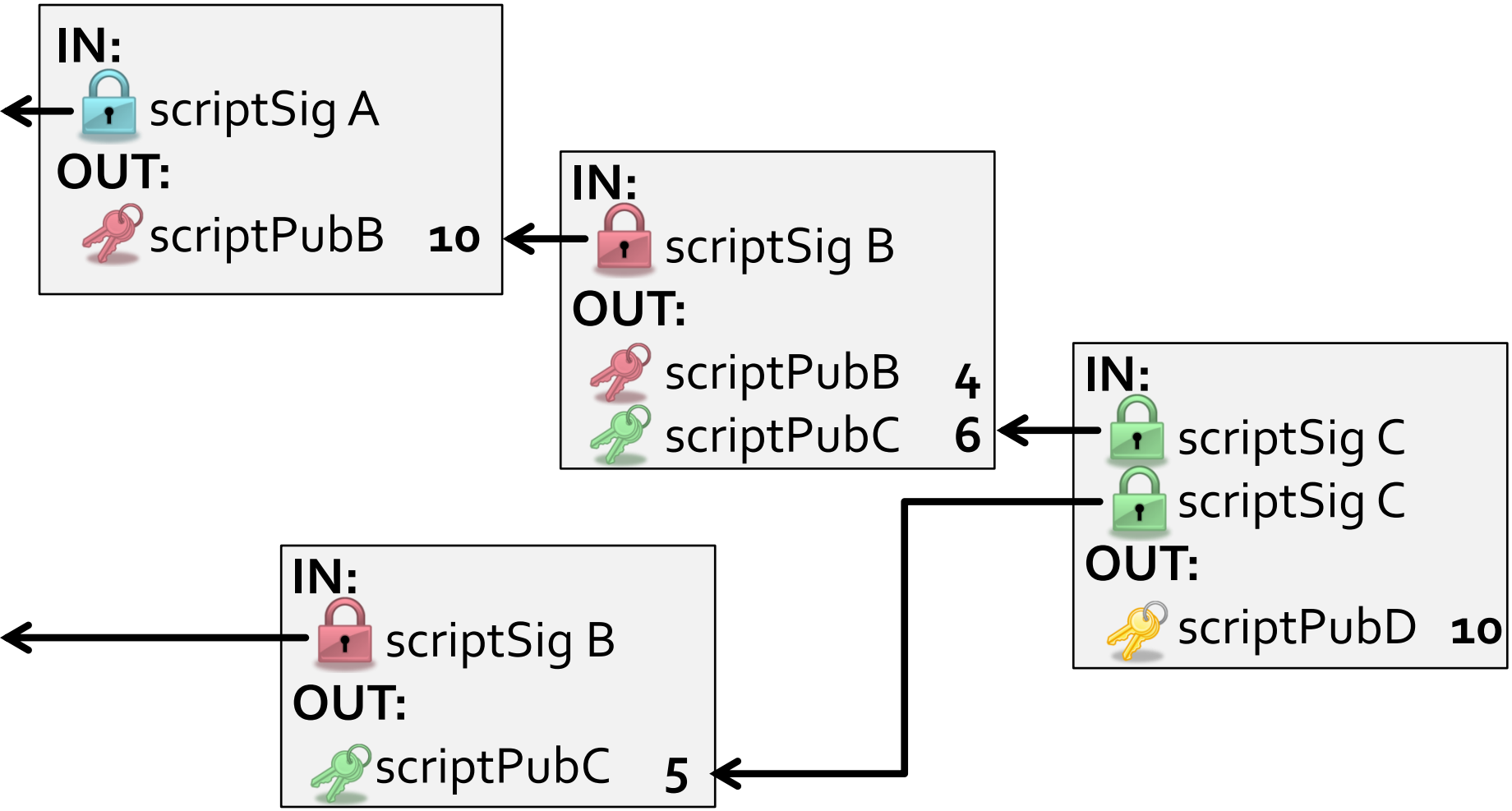
Double spends?



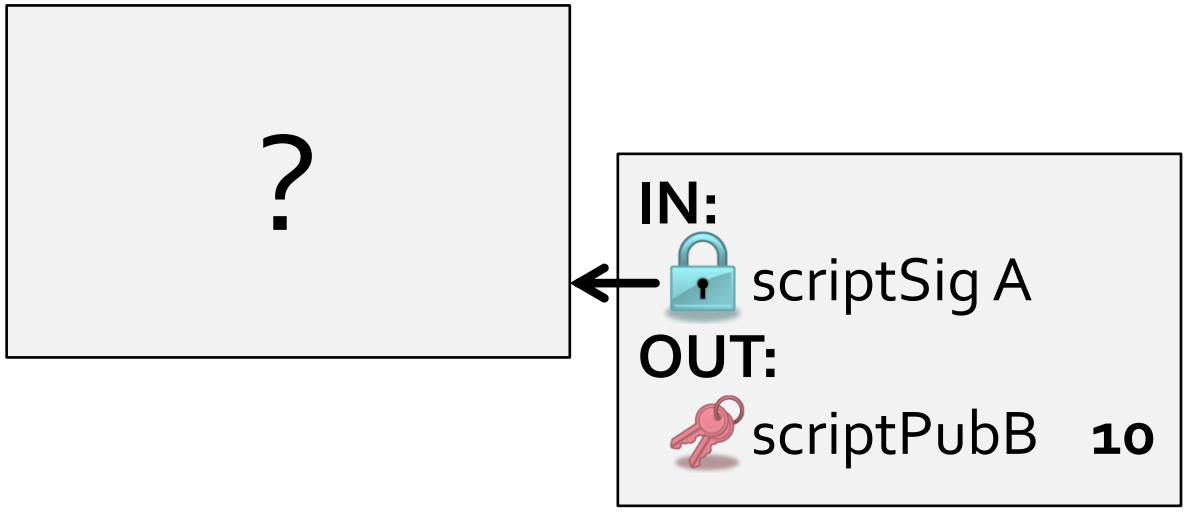
Blockchain Fork



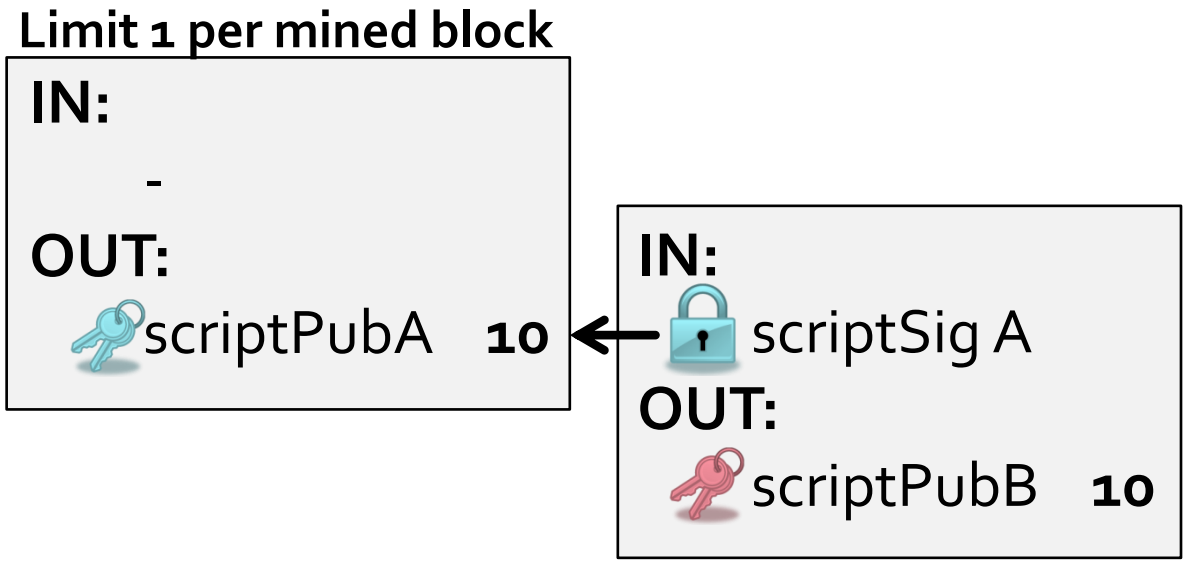
Bitcoin Transactions



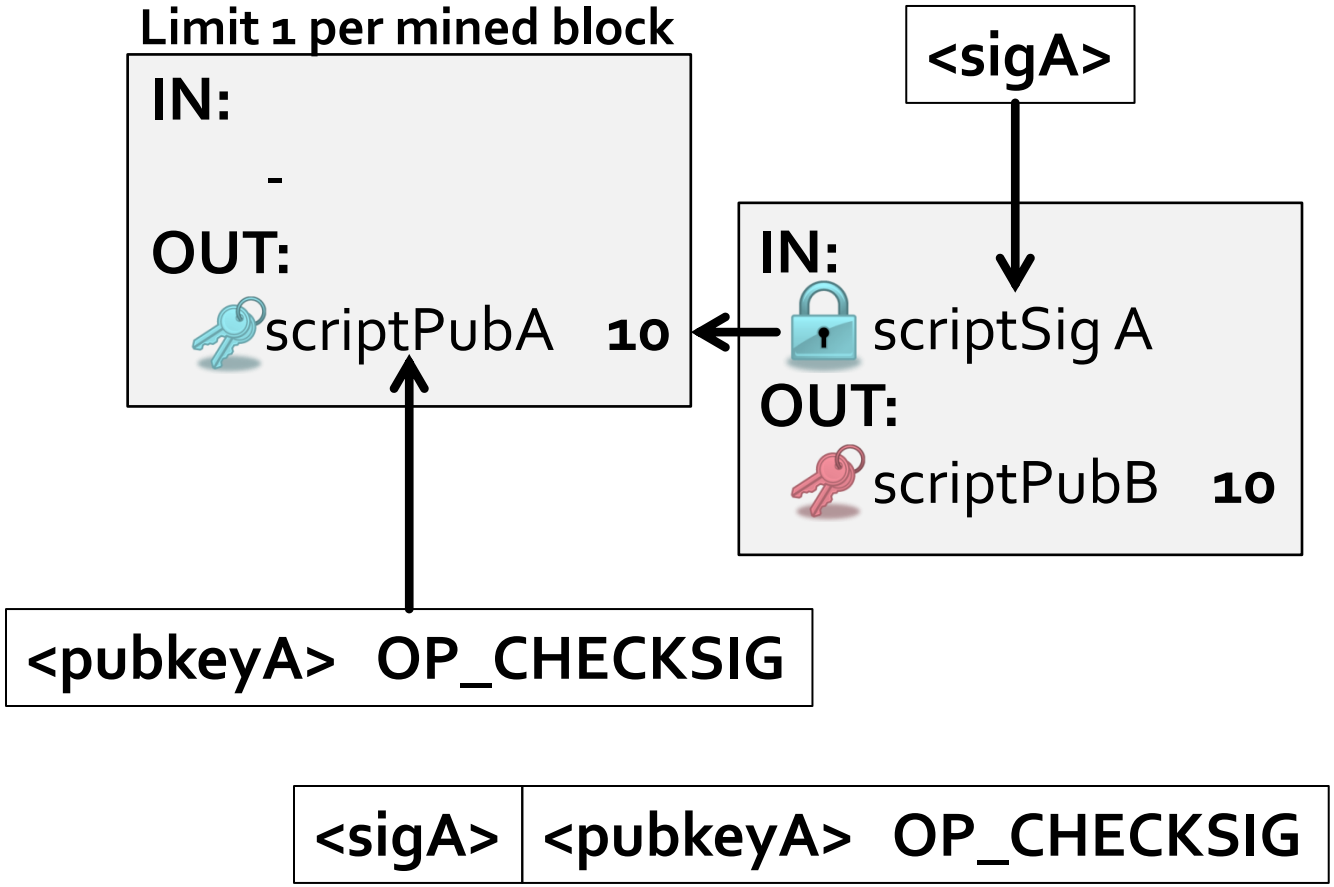
Coinbase transactions



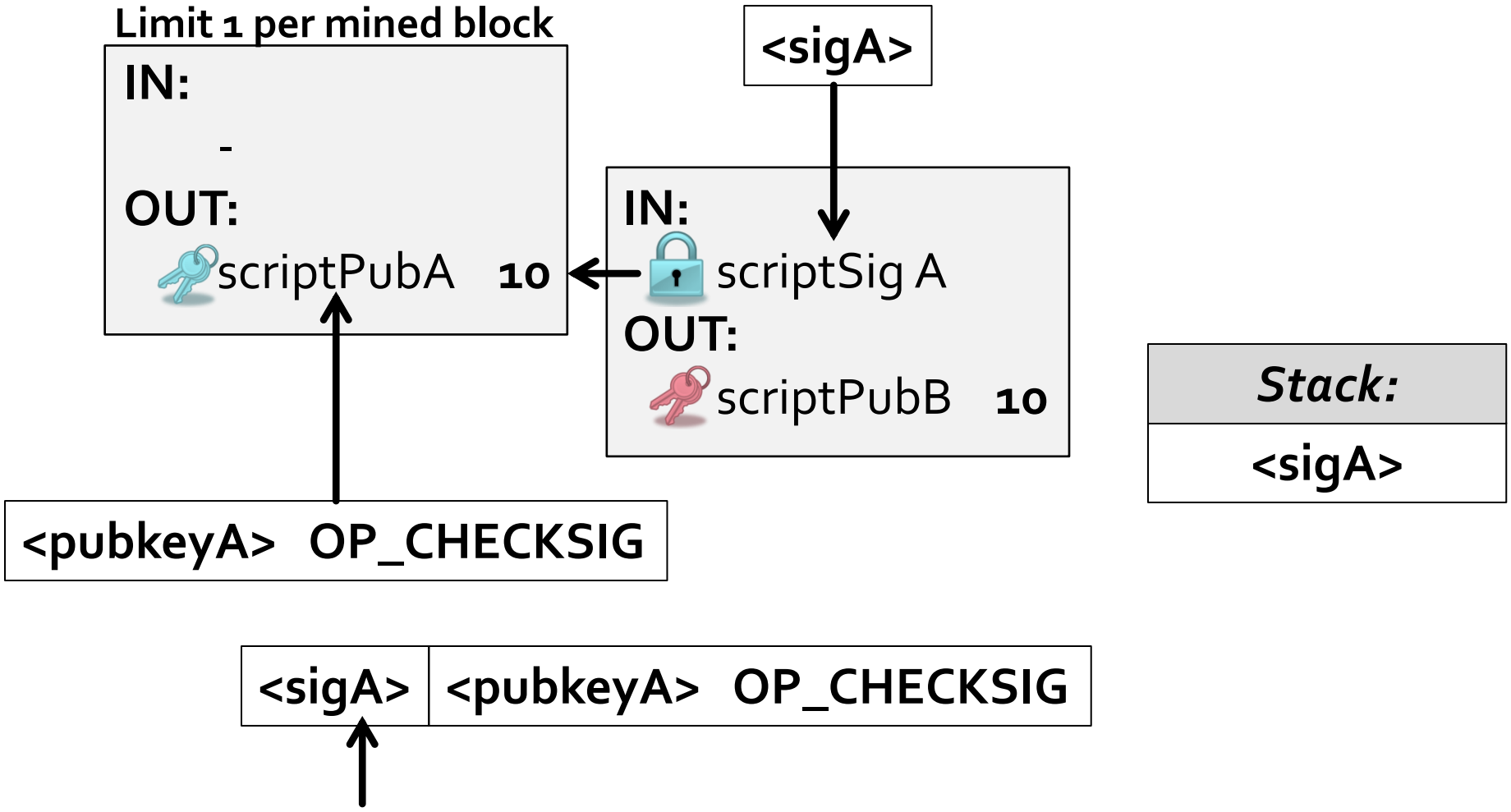
Coinbase transactions



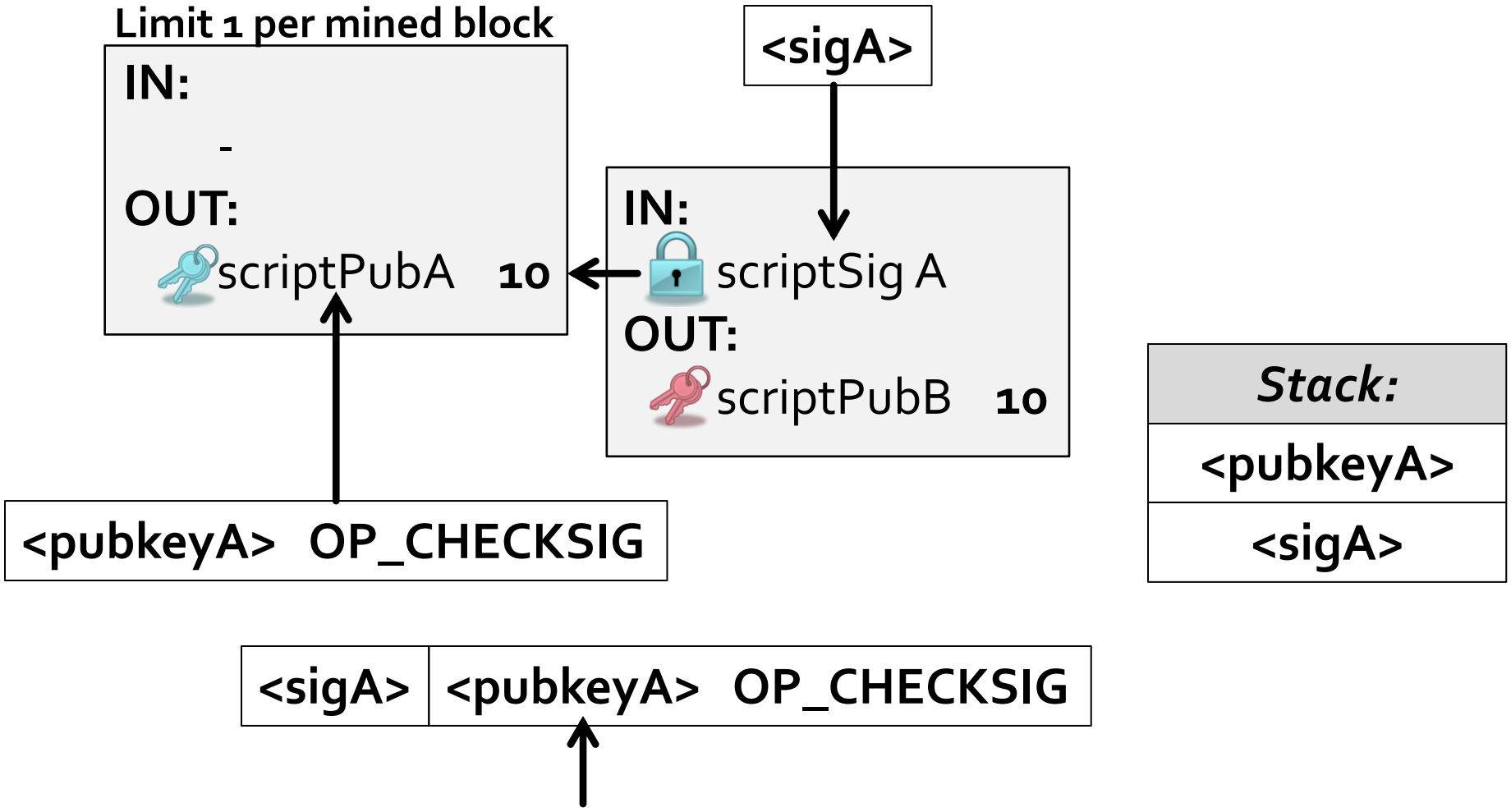
Bitcoin transactions are scripts



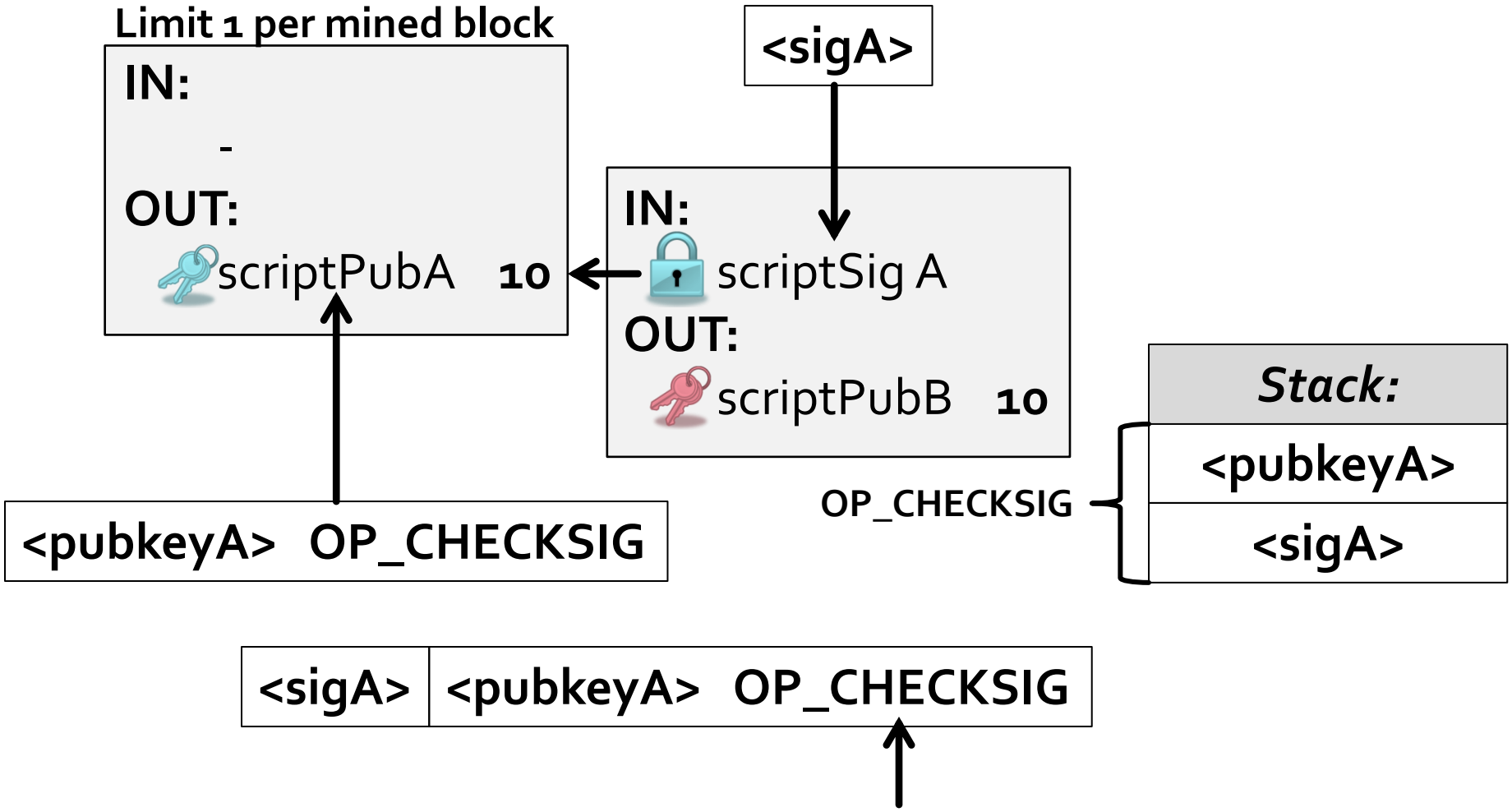
Bitcoin transactions are scripts



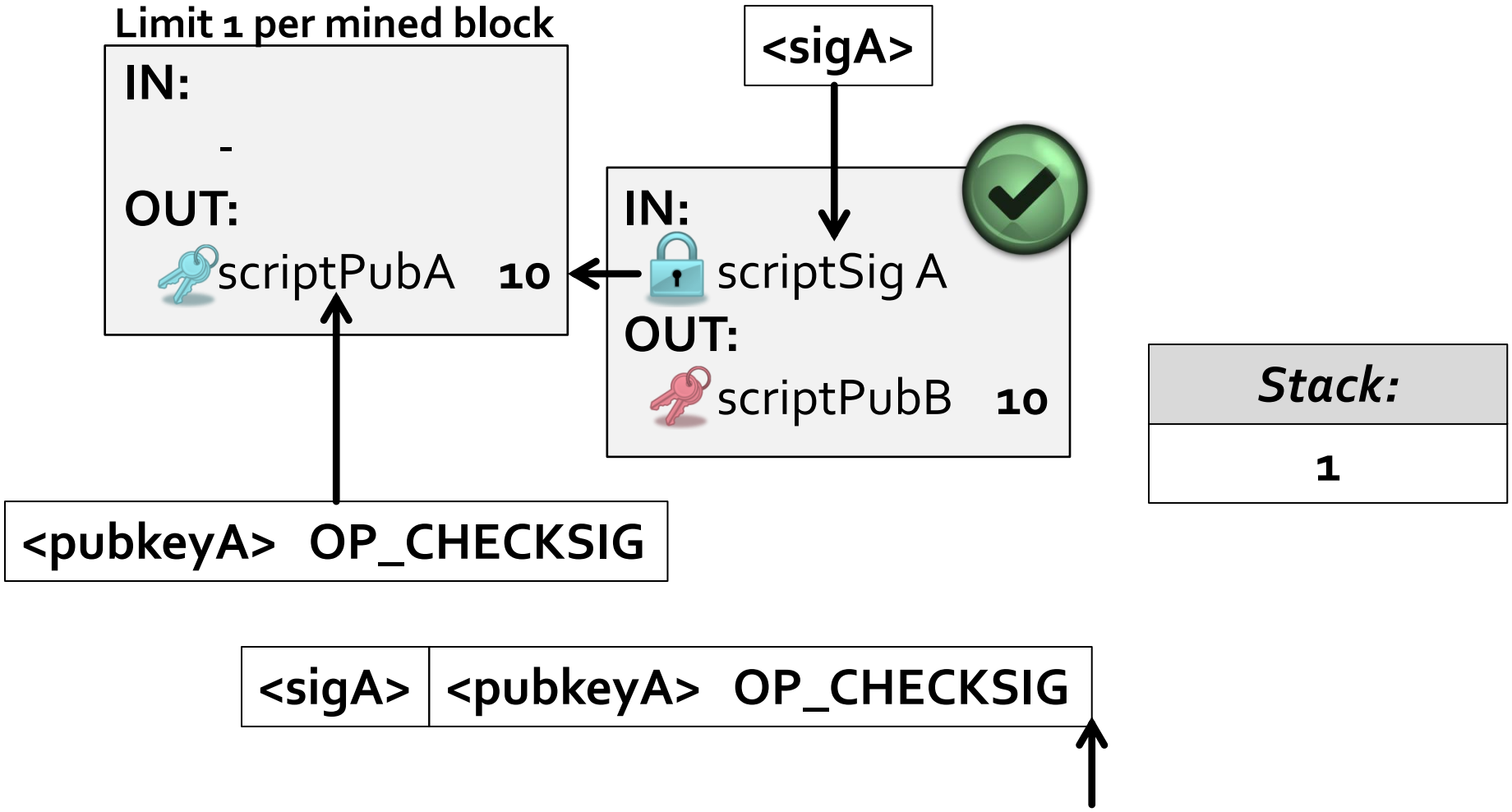
Bitcoin transactions are scripts



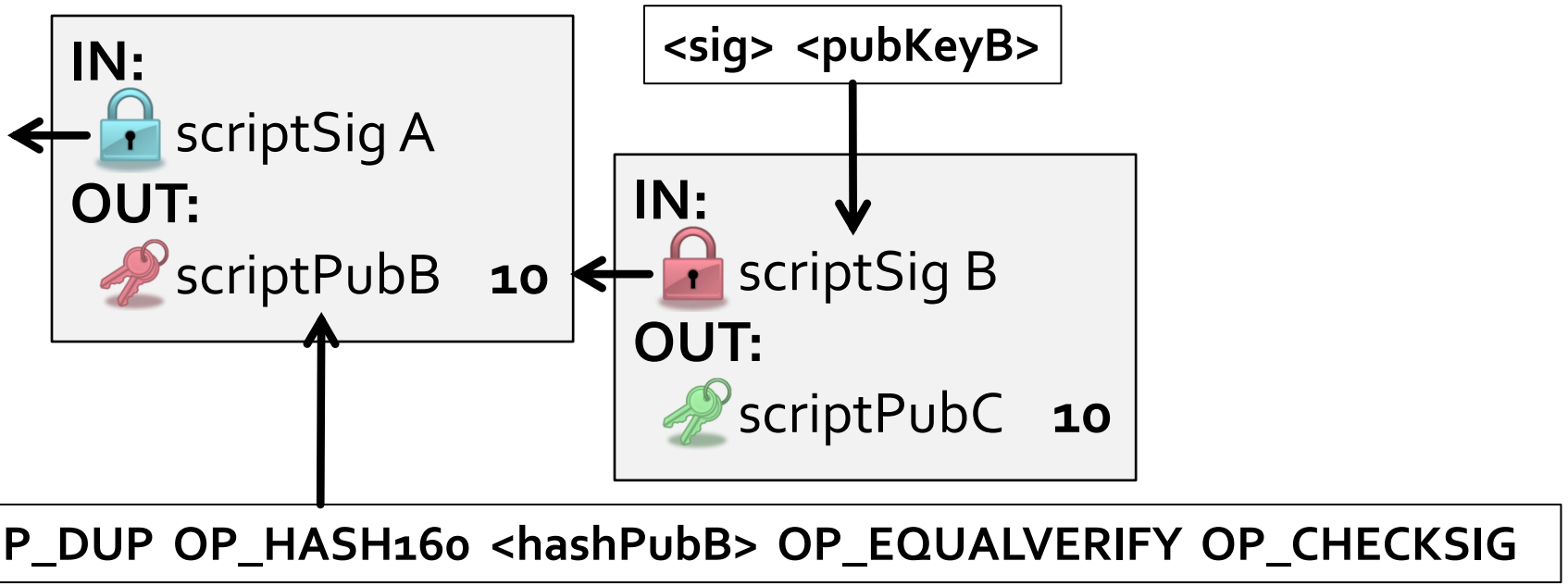
Bitcoin transactions are scripts



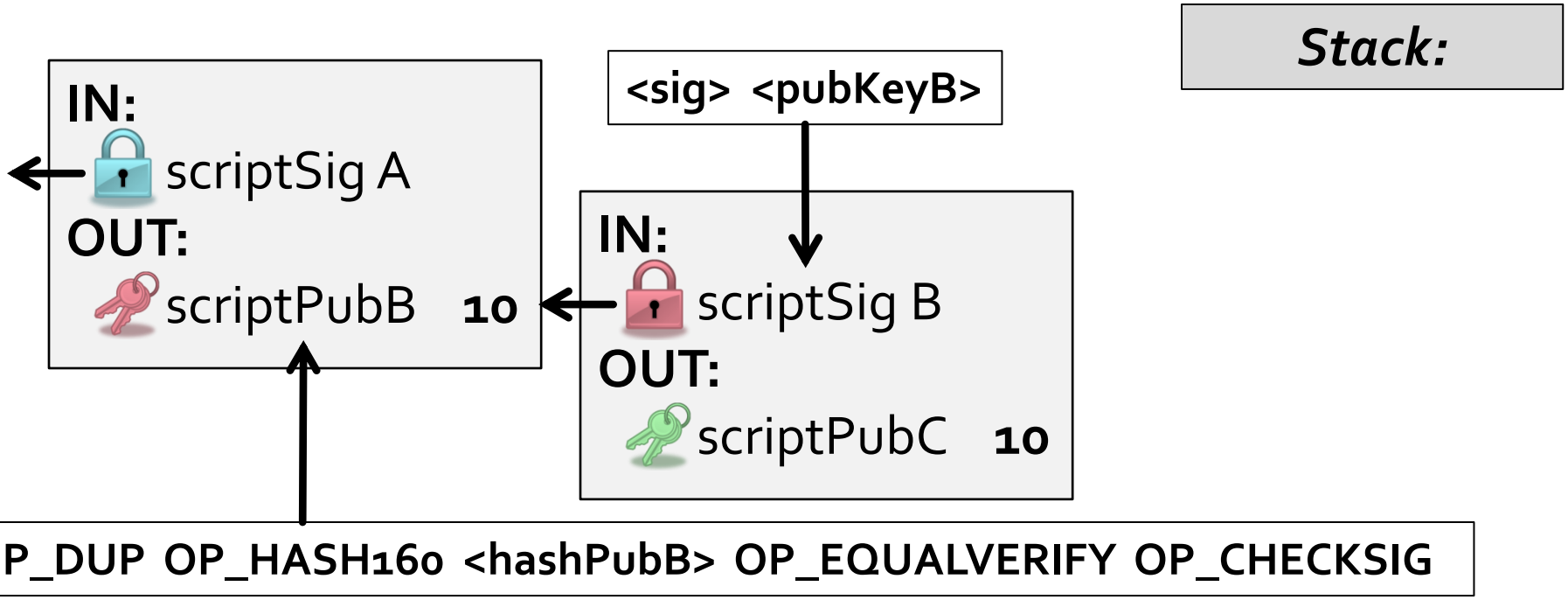
Bitcoin transactions are scripts



"Standard" Bitcoin TX scripts

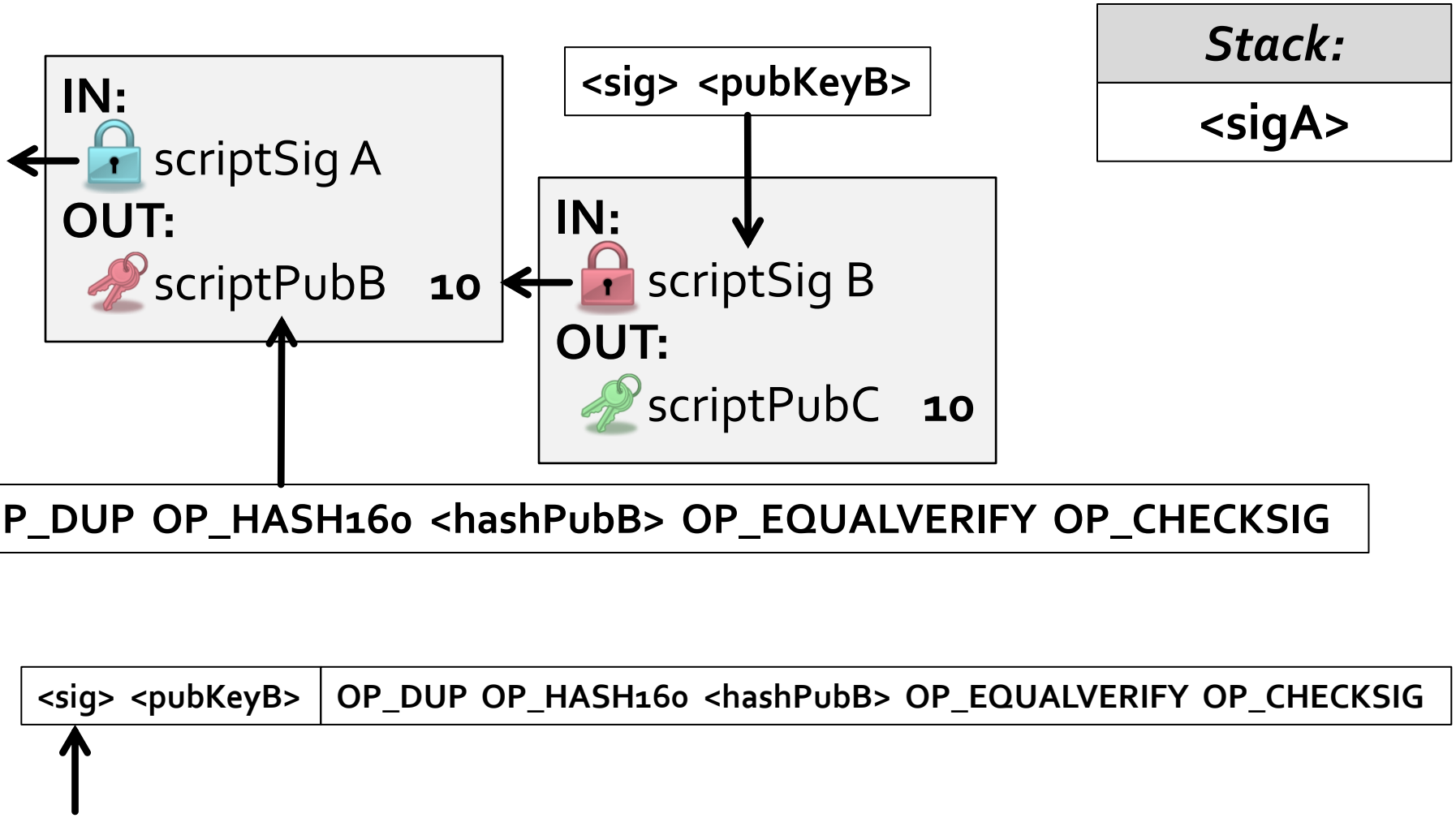


"Standard" Bitcoin TX scripts

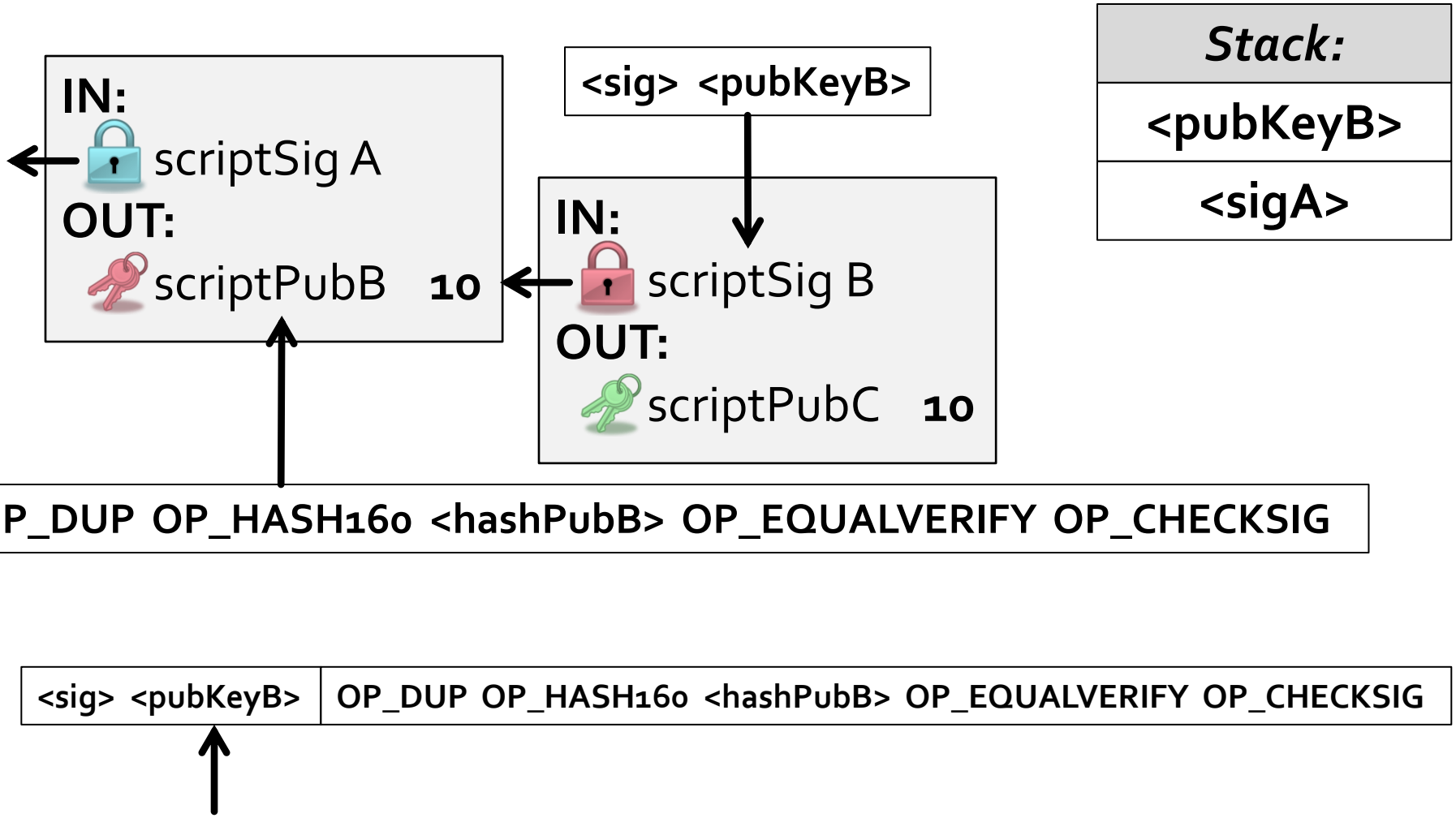


<sig> <pubKeyB>	OP_DUP OP_HASH160 <hashPubB> OP_EQUALVERIFY OP_CHECKSIG

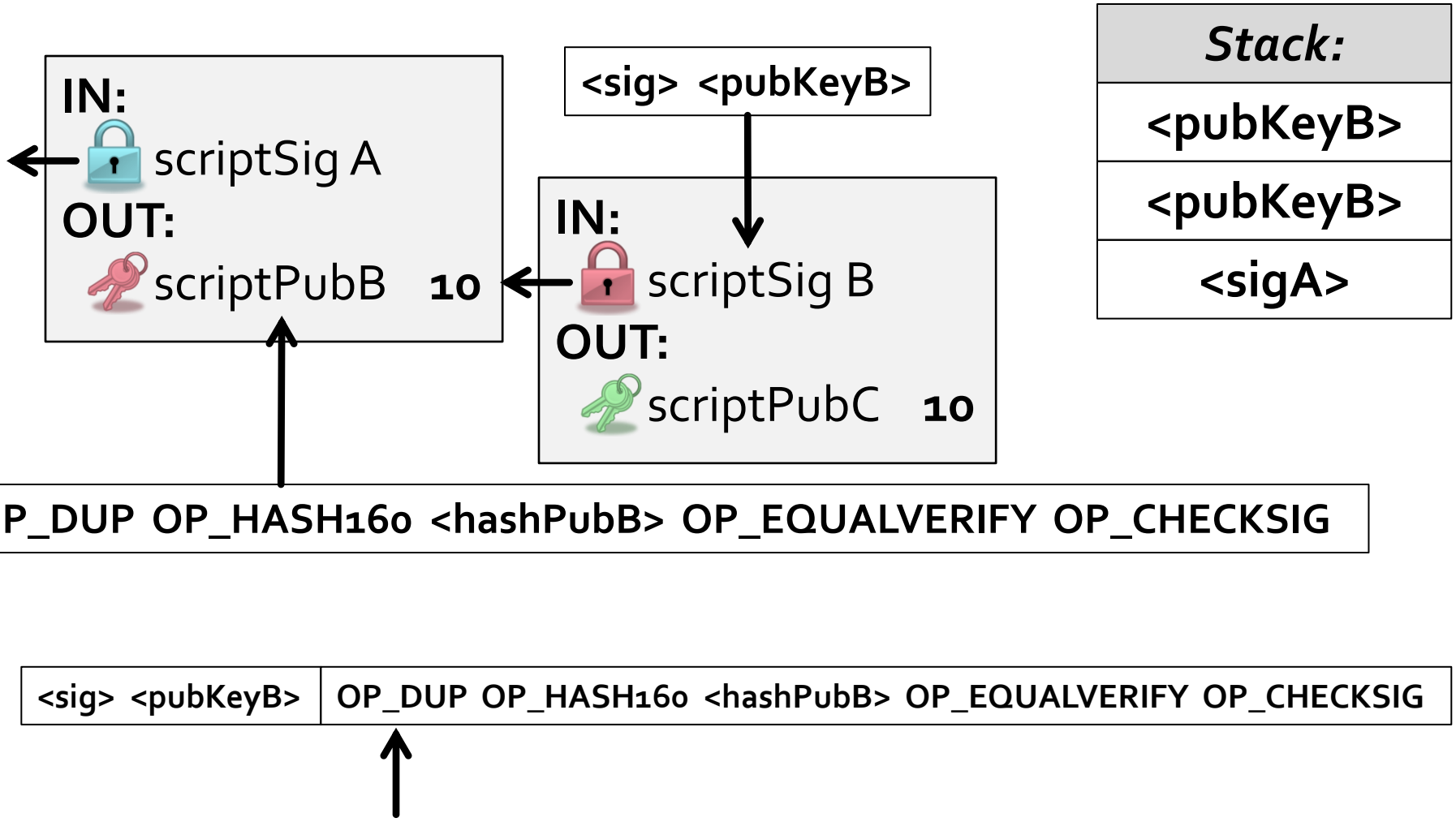
"Standard" Bitcoin TX scripts



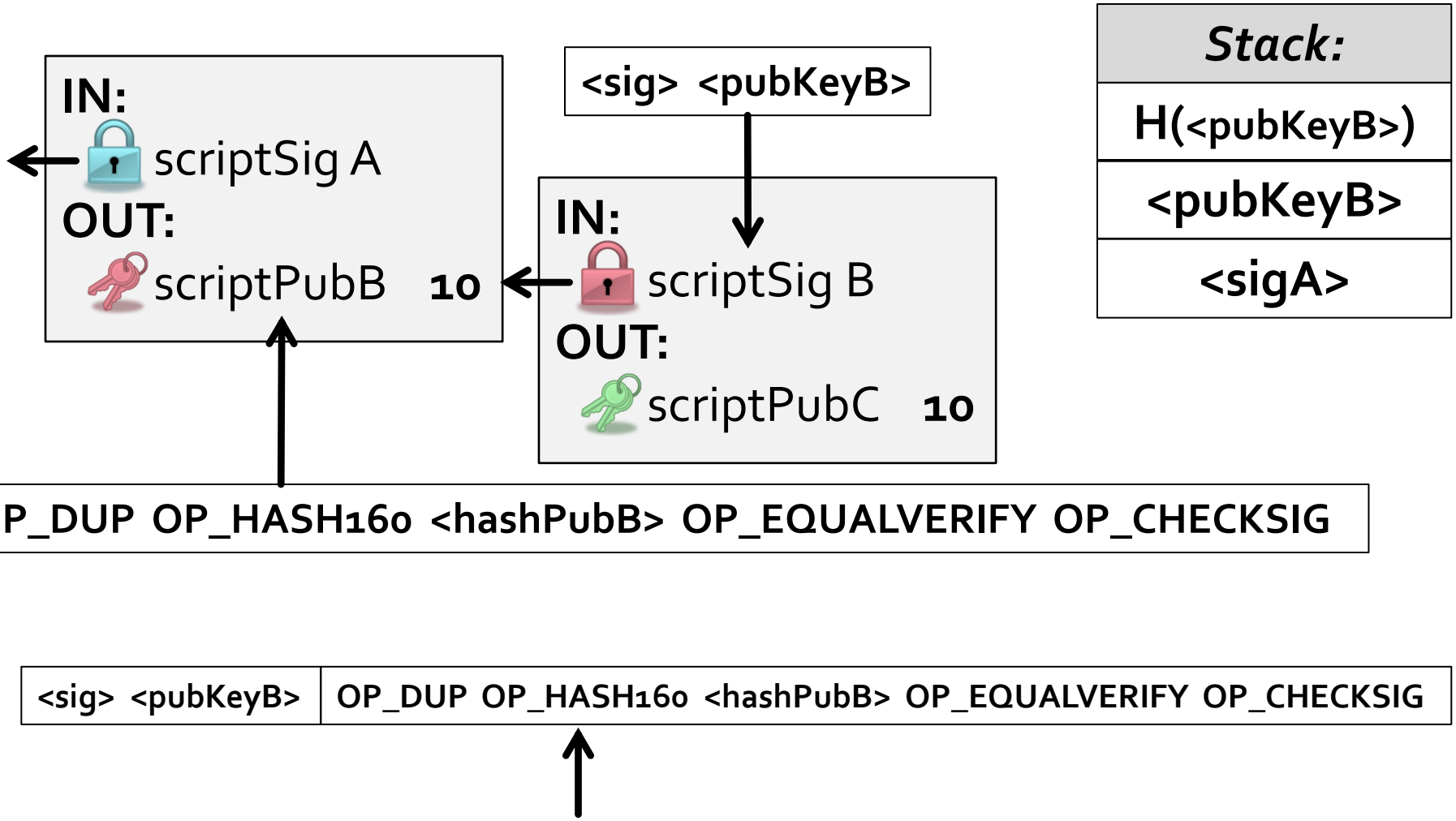
"Standard" Bitcoin TX scripts



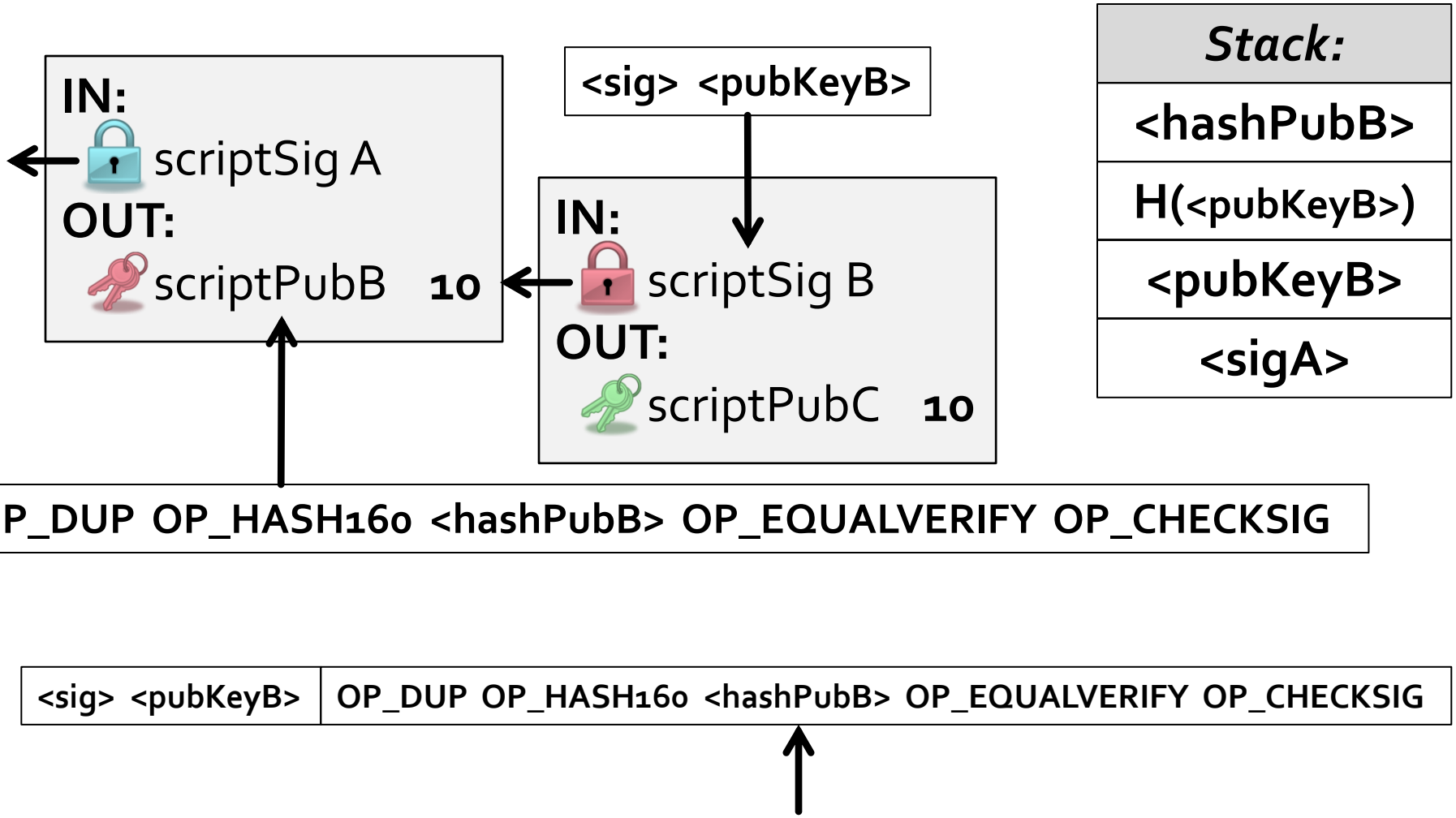
"Standard" Bitcoin TX scripts



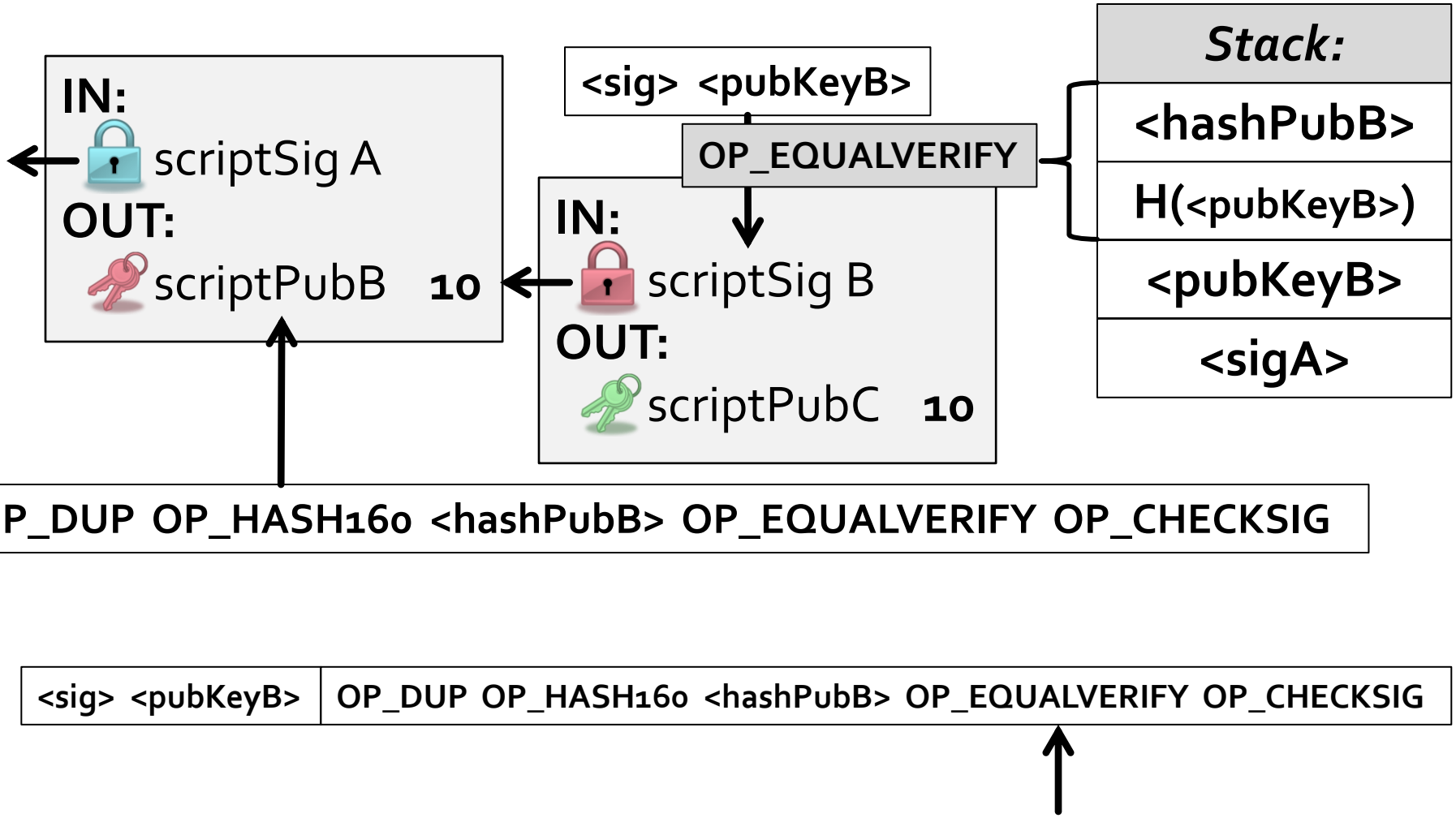
"Standard" Bitcoin TX scripts



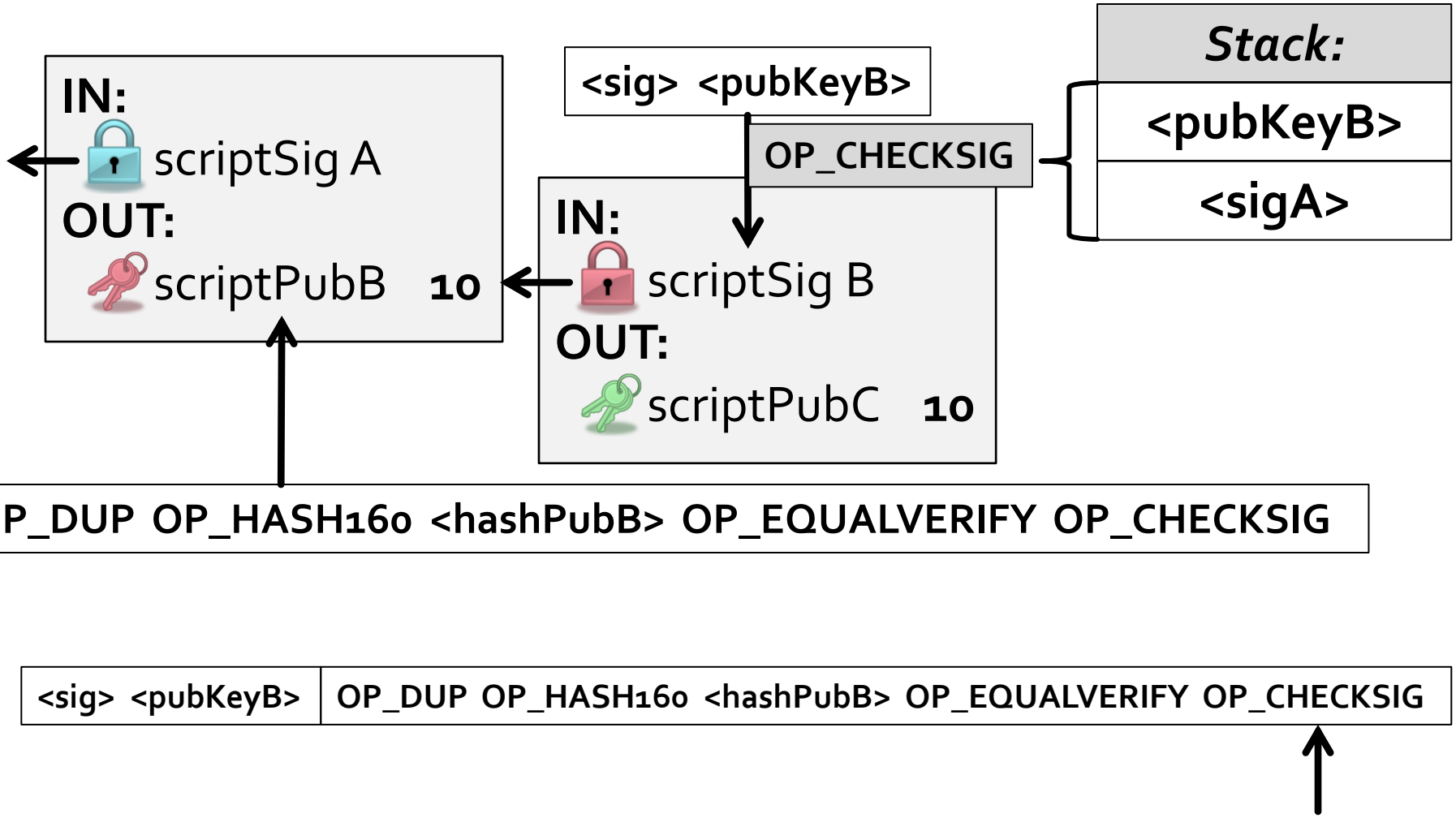
"Standard" Bitcoin TX scripts



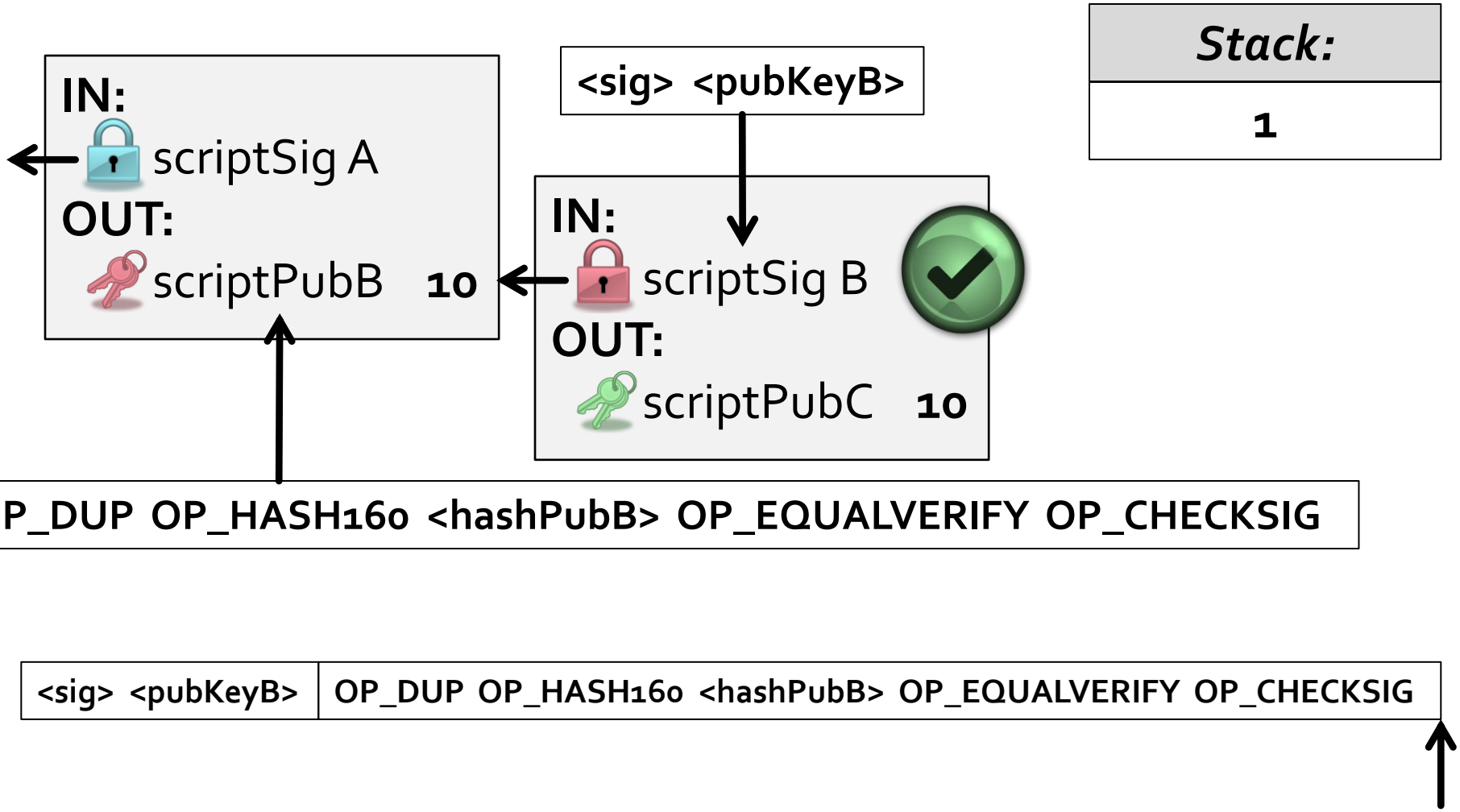
"Standard" Bitcoin TX scripts



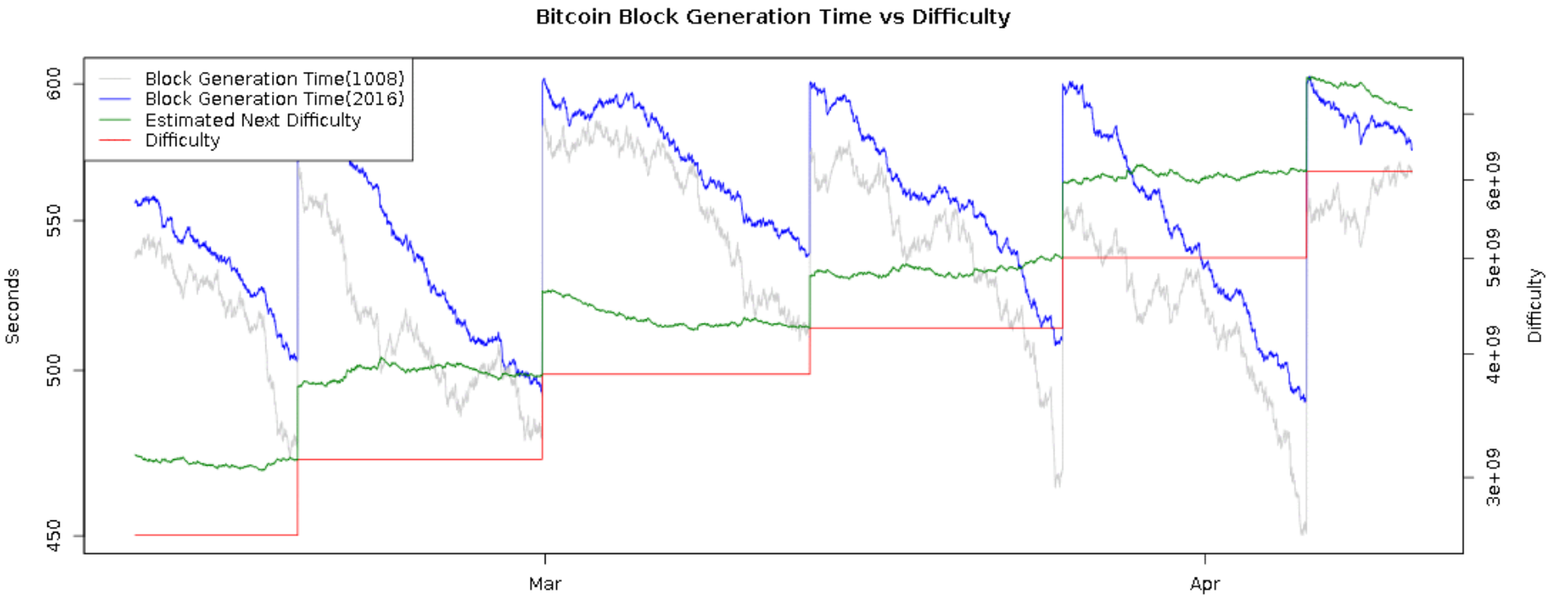
"Standard" Bitcoin TX scripts



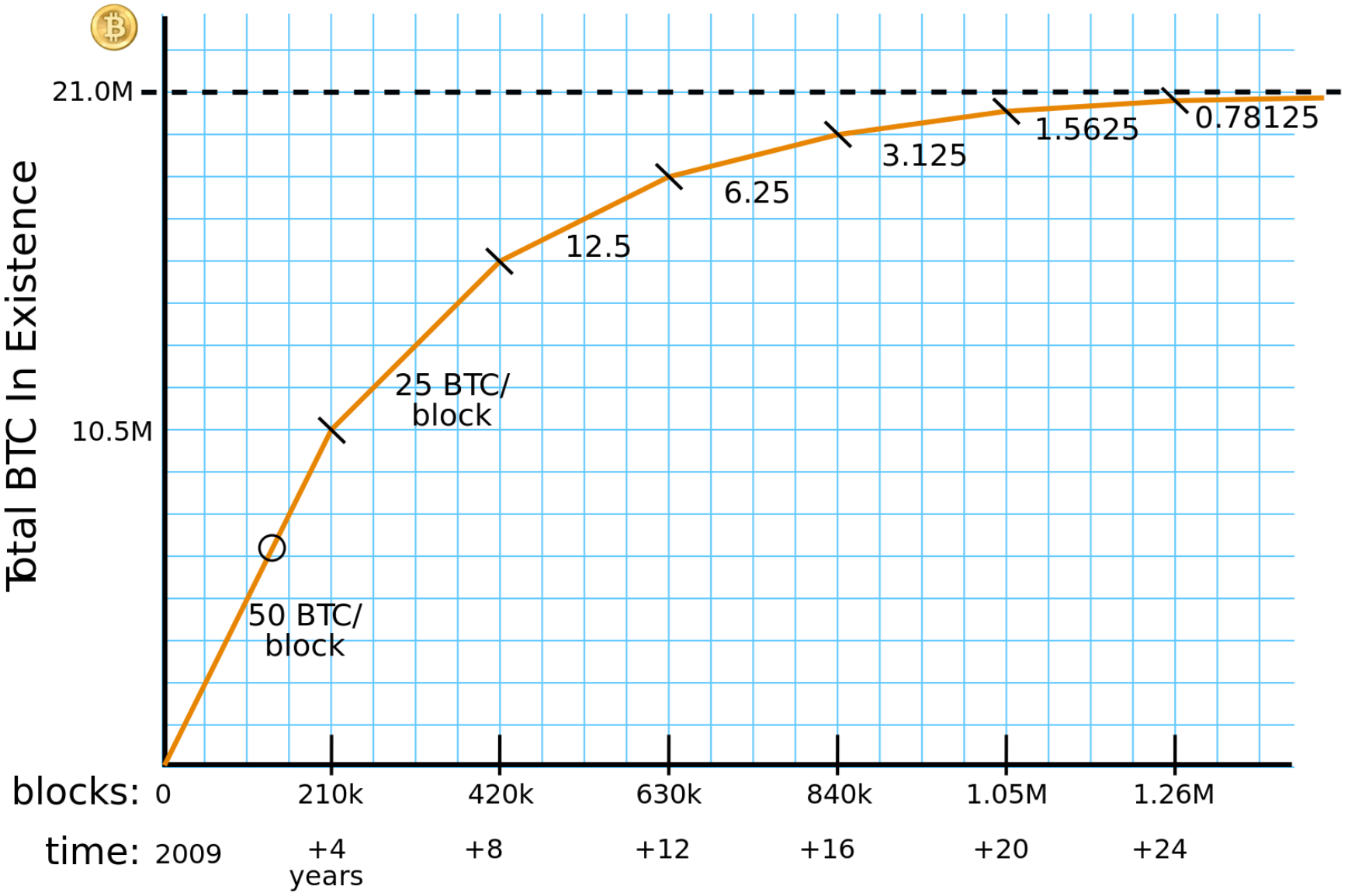
"Standard" Bitcoin TX scripts



Difficulty Adjustment



Mining Reward



Mining difficulty

5 TH/s =~ $5000

45,718 / 5 =
avg. **9144 blocks** to get
25 BTC =

64 days

…if net hash rate is constant…

45,718 TH/s!!!

Total Mining hashrate

4.5 TH/s =~ $2900

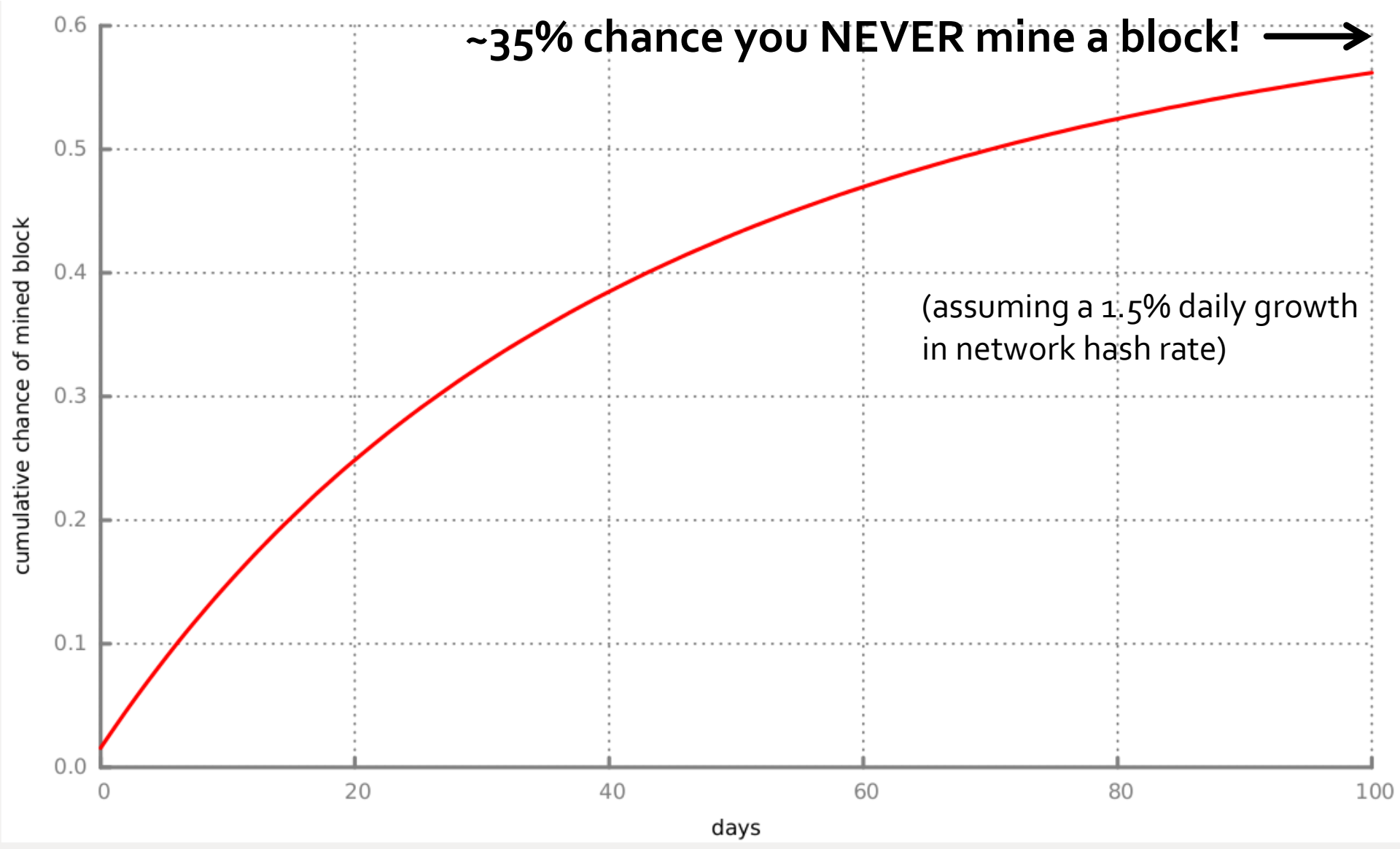
355,792 / 4.5 =
avg. **79,065 blocks** to get
25 BTC =

1.5 year

if hash rate is constant…

355,792 TH/s!!!

Pooled Mining

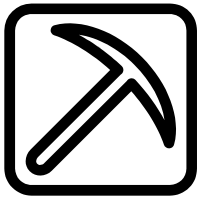


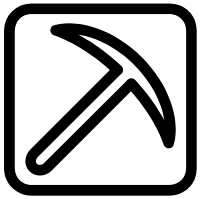
Pooled Mining

Target:
00000000f8c700…
Pubkey:
1FxCNAGBStZkne7…

000000849fed1…
00000032776ea…
00000050b9caf…

00000005111cf95…
00000000c2654d…





Pooled Mining

15 BTC

10 BTC

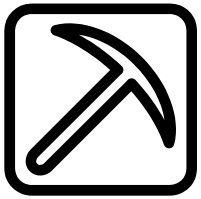
00000084 9fed1…

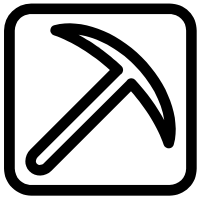
00000032 776ea…

00000050 b9caf…

00000005 111cf95…

00000000 c2654d…





Pooled Mining

Last Blocks

BTC NMC IXC DVC

ID	Completed	Block	฿ Value	Status	Duration	Hash Rate	Your Shares	Score	Total Work	Payout
10622					44 minutes	13.06 Ph/s	0/0	0.00%	8037587372	-
10621	2014-04-10 10:15:48	295089	฿25.0162	6/120	an hour	12.90 Ph/s	4256/5000006979	0.00%	10198927560	฿0.00002129
10620	2014-04-10 09:19:13	295078	฿25.1332	17/120	an hour	12.98 Ph/s	4016/5000003620	0.00%	12664147584	฿0.00002018
10619	2014-04-10 08:09:23	295069	฿25.0776	26/120	13 minutes	12.90 Ph/s	3904/5000003495	0.00%	2253289100	฿0.00001958
10618	2014-04-10 07:56:54	295067	฿25.0236	28/120	a minute	12.49 Ph/s	3776/5000006206	0.00%	221024197	฿0.00001889
10617	2014-04-10 07:55:38	295066	฿25.0994	29/120	8 minutes	12.99 Ph/s	3776/5000006206	0.00%	1493769887	฿0.00001895
10616	2014-04-10 07:47:24	295065	฿25.1971	30/120	2 hours	12.94 Ph/s	3920/5000005812	0.00%	20670193325	฿0.00001975
10615	2014-04-10 05:53:05	295052	฿25.1689	43/120	2 hours	12.96 Ph/s	4544/5000006914	0.00%	20623464450	฿0.00002287
10614	2014-04-10 03:59:08	295045	฿25.0276	50/120	an hour	12.92 Ph/s	4032/5000004334	0.00%	14180372412	฿0.00002018
10613	2014-04-10 02:40:34	295036	฿25.1044	59/120	30 minutes	12.98 Ph/s	3888/5000004408	0.00%	5421429660	฿0.00001952
10612	2014-04-10 02:10:40	295032	฿25.0597	63/120	2 minutes	12.56 Ph/s	4352/5000004514	0.00%	318700394	฿0.00002181
10611	2014-04-10 02:08:51	295031	฿25.1667	64/120	32 minutes	13.03 Ph/s	4352/5000004514	0.00%	5755748654	฿0.00002190
10610	2014-04-10 01:37:14	295029	฿25.0088	66/120	an hour	13.00 Ph/s	3856/5000003095	0.00%	12695151551	฿0.00001928

Example mining return (~11 GH/s)