LIGHTNING NETWORK

on blockchain

FUNDING TXN (CREATE CHANNEL)

TERMINATES CHANNEL

should split money acc. to latest balances (A:9, B:6)

punishment transaction

time

challenge period

2 parties

A, B

5 10 BTC

Locks (INITIAL AMOUNTS)

A 3 | A 8

B 12 | B 7

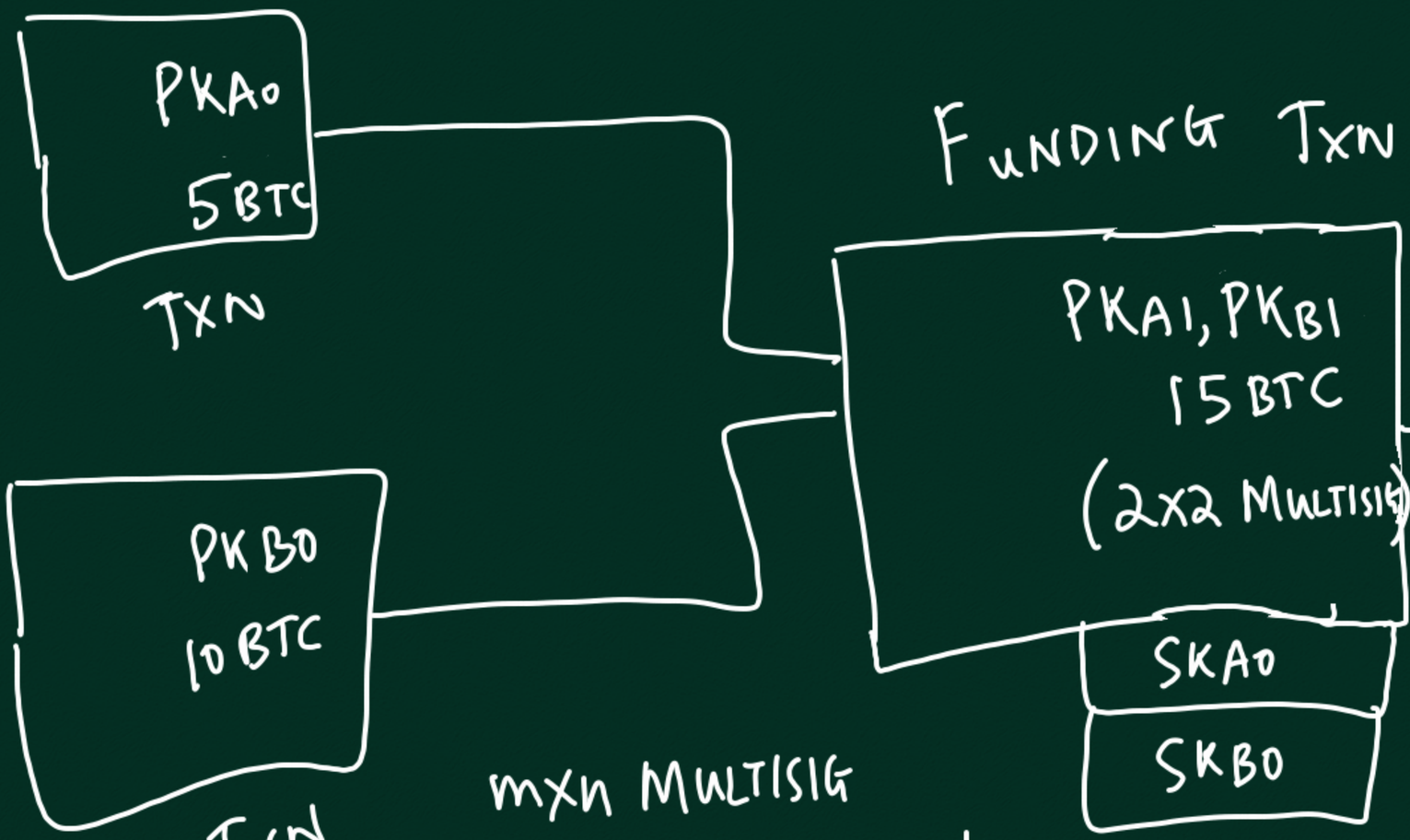
A 9 → BAL

B 6 → BAL

If split is not acc. latest balance, honest party punishes guilty one, and takes full amount (15 BTC)

Funding Transaction

A: 9
B: 6



mxn Multisig

$\Rightarrow$ n keys, any txn signed by any 'm' secret keys (among 'n' keys) can spend output

Attendance

1) Create templates (w/o Signatures) of

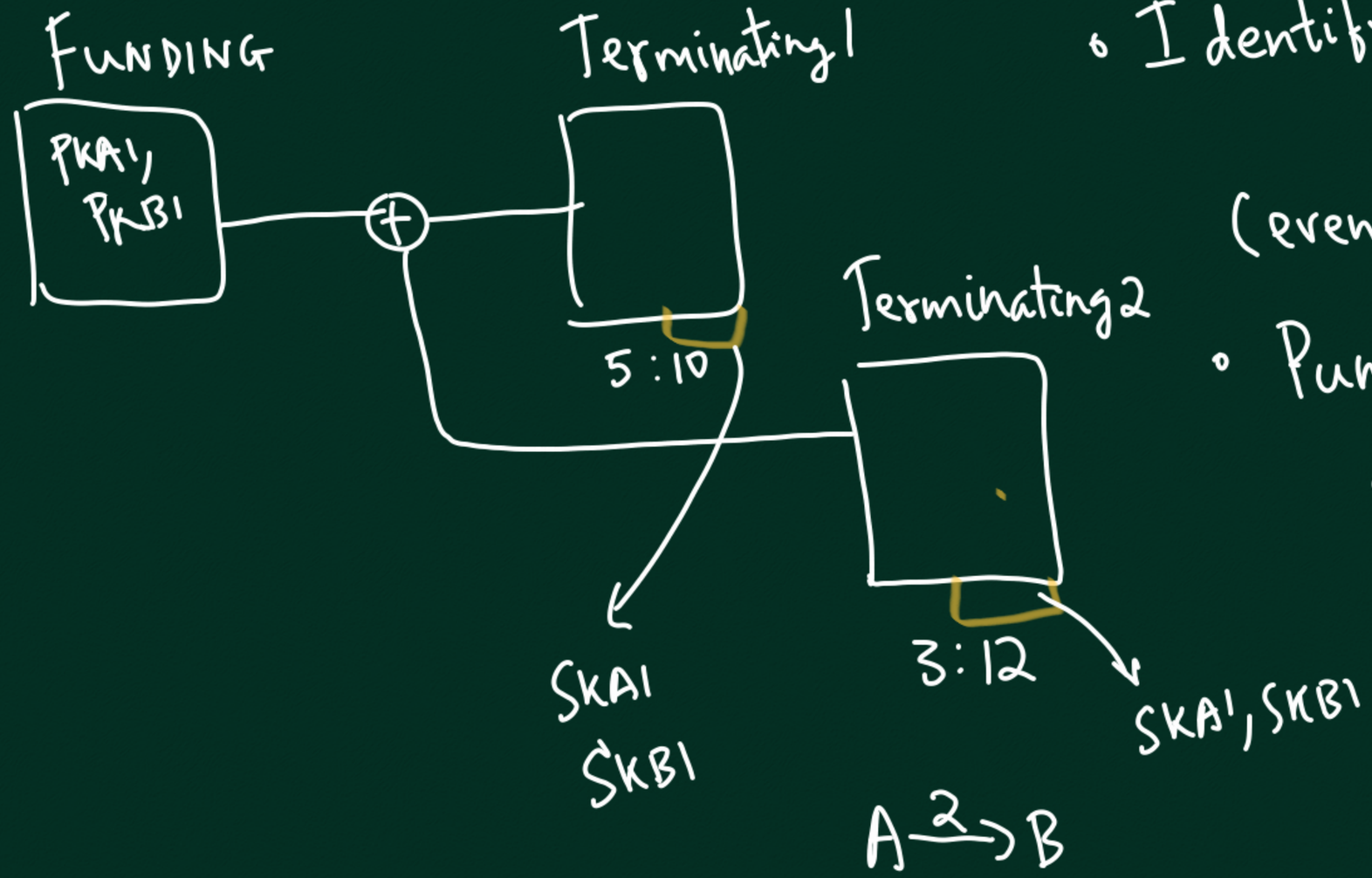
- Funding txn.
- Terminating txn

with public keys for o/p etc

2) Sign Terminating txn ⟷ give to other party

3) Sign Funding Txn ⟷ give to other party

4) Put Funding txn on blockchain



Want

- Identify old terminating txn (even indirect manner)
- Punish whoever sent old txn

COMMITTMENT → Full signed, only with C1a

A: 5, B: 10

FUNDING

PKA1, PKB1

2×2

Outputs

0: 5 BTC RSMC(PKA2, PKB3)

1: 10 BTC PKB2

SKB1 → Half signed

C2a

C2b

0: 10 for B

1: 5 for A

C1b | SKA1

While creating C2a, C2b

A gives SKA2 to B

So B can punish A if C1a goes on-chain, as B has both keys of RSMC

- Create Funding txn template (involves exch. of some info)
- Create C1a, C1b templates. Exchange half-signed C1a, C1b
- A creates fully signed C1a LOCALLY (Similar for B)
- Exch. Signatures for Funding txn and put it on blockchain

Revocable Sequence Maturity Contract

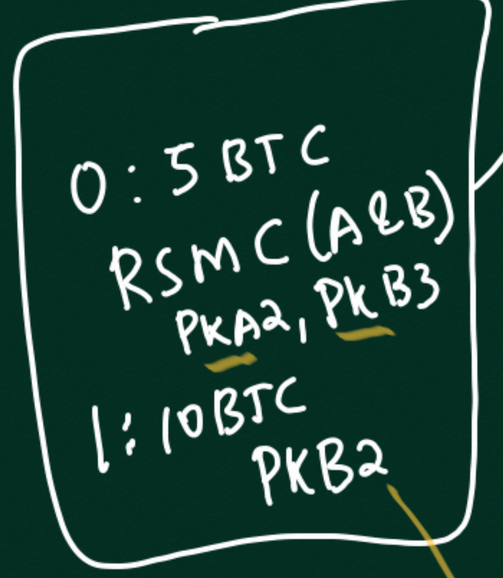
C1a C2a

A:3

B:12

C1b C2b

C1a



Output can be spent

- At any time by txn signed by SKA2 and SKB3
- After 1000 blocks by txn signed by SKA2

punishment time window

JQWXQKBE