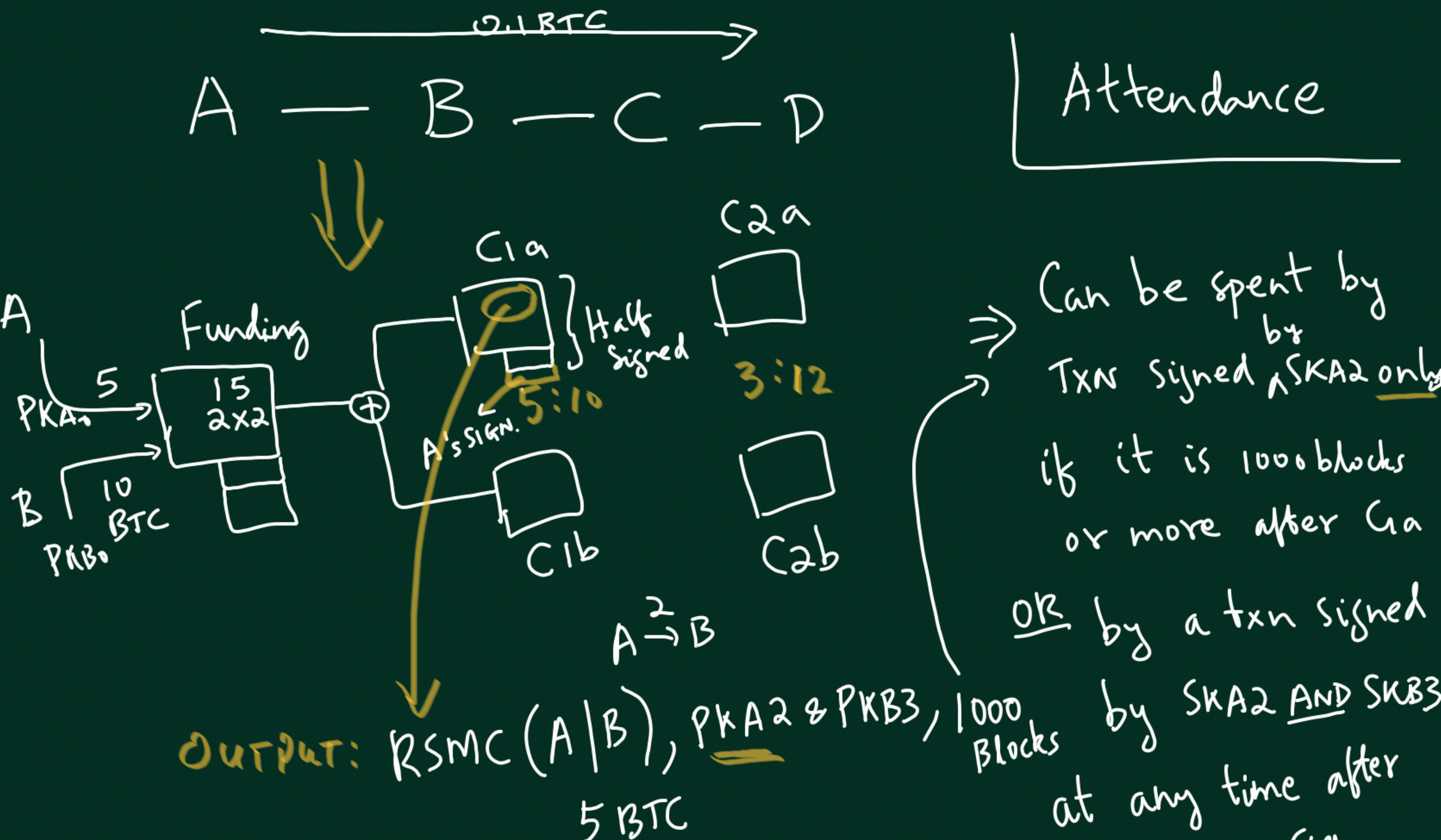
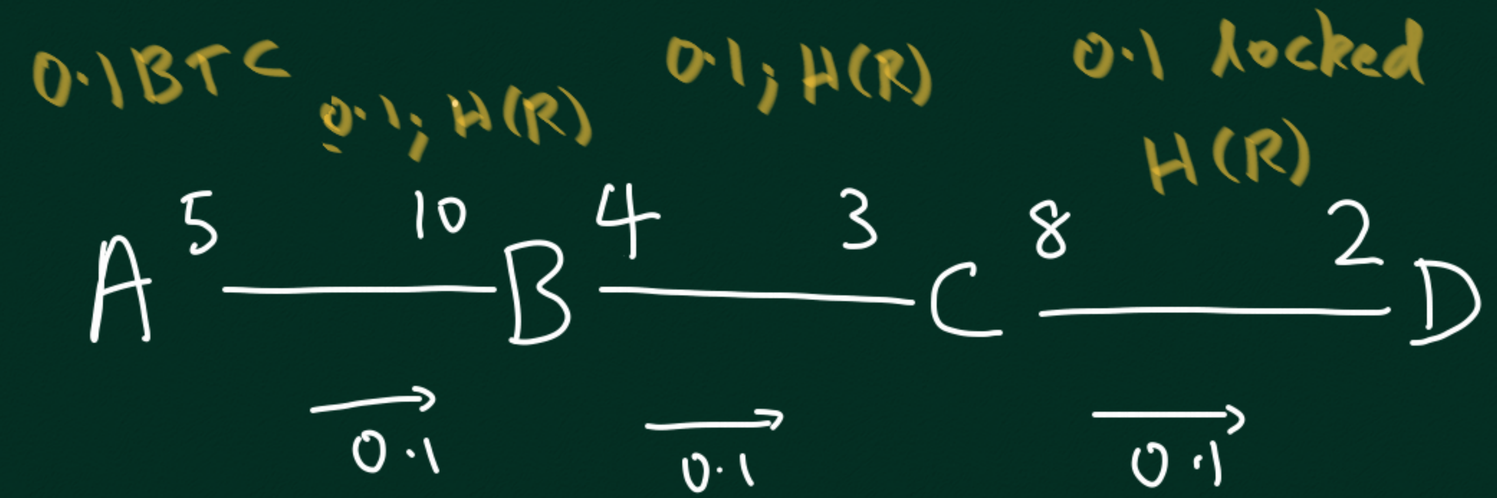

2.1 BTC
A — B — C — D
Attendance
A
Funding
5
PKA
15
2x2
B
10
BTC
PKB
C1a
Half signed
A's SIGN.
5:10
C1b
C2a
3:12
C2b
A ⇄ B
OUTPUT: RSMC (A|B), PKA2 & PKB3, 1000 Blocks
5 BTC
⇒ Can be spent by
by
Txn Signed ^SKA2 only
if it is 1000 blocks
or more after C1a
OR by a txn signed
by SKA2 AND SKB3
at any time after
C1a



① Timing

② How to connect channel states across multiple P.C.s → Using common secret.

R
secret

H(R)
hash

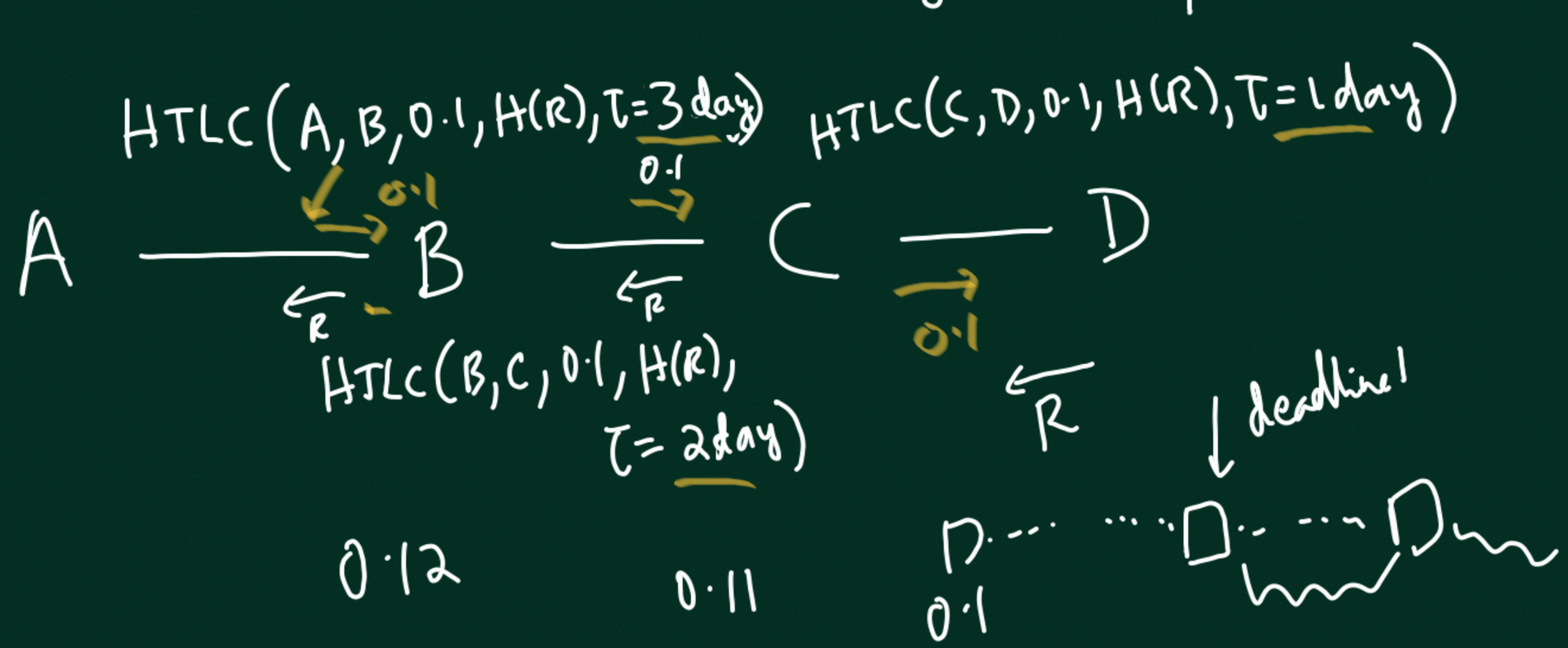
placed in contract

If R revealed, then some action (e.g. payment) takes place

HTLC: Hash Time-Lock Contract

C1a C2a
C1b C2b

Ex: A locks 0.1 BTC for B
Secret: H(R)
For time: $\tau = 1$ day



In Summary

1) A and D get together, A decides to pay D 0.1 BTC

2) D chooses random R; gives H(R) to A

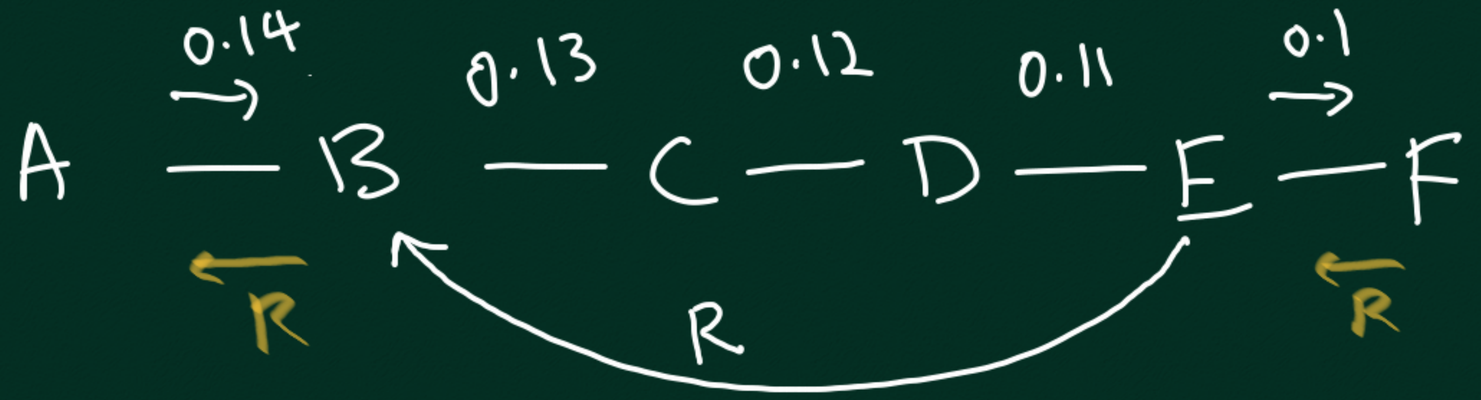
3) A selects path A → B → C → D and finds that 0.1 available on entire path

MICROPAYMENT

4) A sets HTLC(A, B, 0.12, H(R), T = 3 days) with B;
   B sets HTLC(B, C, 0.11, H(R), T = 2 days) with C
   C sets HTLC((, D, 0.1, H(R), T = 1 day) with D

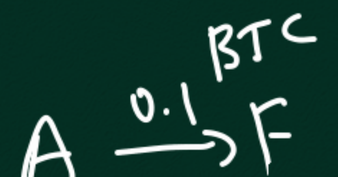
   assuming 0.01 txn fee per hop

5) D reveals R to C before 1 day; C reveals R to B before 2 days;
   B reveals R to A before 3 days



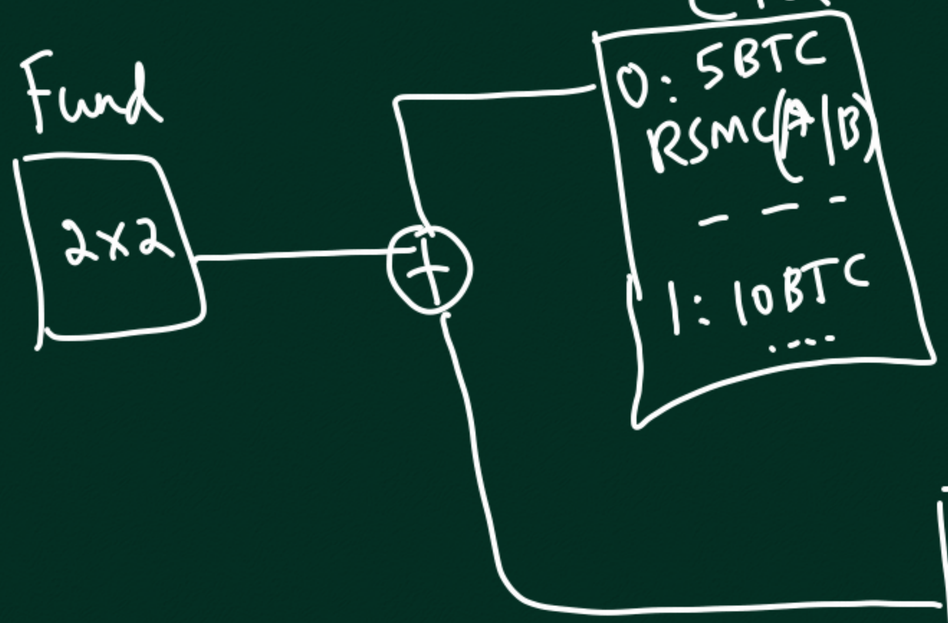
Worm-hole attack

E & B collude



0.04 between them or 0.02 each

Implementation

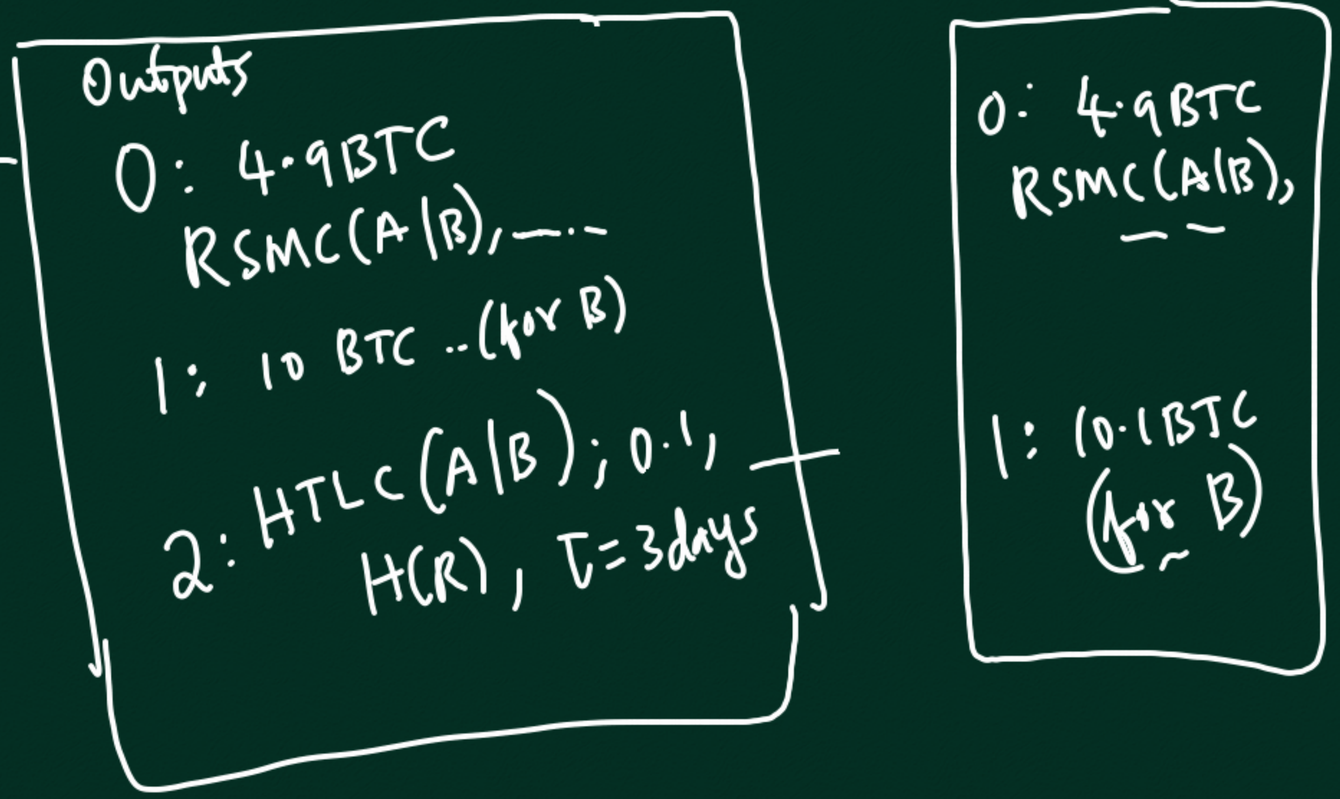


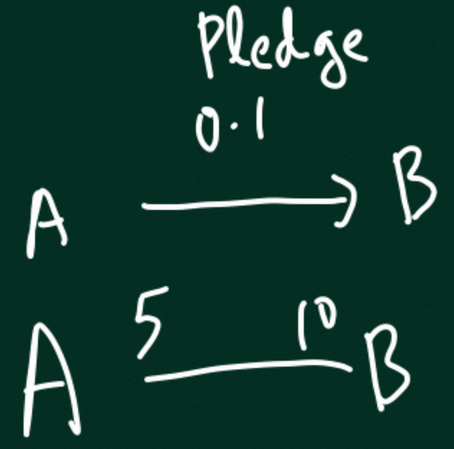
RSMC (A|B) → C1a

RSMC(B|A) → C1b

Suppose B shows R to A before T=3days (off-chain)

⇓ (if A co-operates)





HTIa

Output
0: RSMC(A|B)
0.1 BTC

C2a

0: RSMC (4.9BTC)
1: 10BTC (A or B)
2: HTLC(A|B), 0.1,
H(R), T=3days

Sent by A on-chain after T=3days

(HEDIa)

Output
: 0.1
(for B)
((Contains R)

as RSMC studied earlier

What if C2a is an OLD Commitment??

If C2a is old, then A loses 0.1 in this RSMC

B's sign must be reqd. for this, since B must know RSMC contents

C3a, C4a, C5a ....

A must approve contents, hence A's sign reqd. for this

Suppose A puts C2a on-chain and B learns R before T=3days

Q1 how to enforce?

Sent by B on-chain before T=3days

Implementation of HTLC (A|B) 0.1 BTC, 3 days

(Can be spent in 2 ways)

mentioned in HTLC output

$H(R)$; P'_{A2} AND P'_{B2} → any txn with R and signed by SK'_{A2} and SK'_{B2} (e.g. HE01a)

OR

P'_{A1} AND P'_{B1} → any txn signed by SK'_{A1} and SK'_{B1}

(e.g. HT1a)

Ethereum

(1) Rollups → ZK-proof rollups

(1) Rollups → Optimistic rollups

(2) Raiden Network (P.C.N.)