Lightning Network

HKU

Cai Cailing

Abstract

The bitcoin protocol can encompass the global financial transaction volume in all electronic payment systems today, without a single custodial third party holding funds or requiring participants to have anything more than a computer using a broadband connection. A decentralized system is proposed whereby transactions are sent over a network of micropayment channels (a.k.a. payment channels or transaction channels) whose transfer of value occurs off-blockchain. If Bitcoin transactions can be signed with a new sighash type that addresses malleability, these transfers may occur between untrusted parties along the transfer route by contracts which, in the event of uncooperative or hostile participants, are enforceable via broadcast over the bitcoin blockchain in the event of uncooperative or hostile participants, through a series of decrementing timelocks.

Lightning Network

Vedio https://www.bilibili.com/video/av18042505/

Proposed 2015/ 02, Joseph Poon, Thaddeus Dryja

<The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments>

Function The Lightning Network is a system of smart contracts built on Bitcoin Blockchain that allows for fast, cheap payments, and reduce transaction fees by keeping them off the main network. It can help Bitcoin be more useful as a day to day currency.

Conceptions RSMC (Recoverable Sequence Maturity Contract)

HTLC (Hashed Timelock Contract)

Framework of Lightning Network

(1) A multi-signature wallet is set up

(2) The wallet address is then saved to the public Bitcoin blockchain including a balance sheet (smart contract) that proves how much of this bitcoin deposits belongs to whom

(3) After this payment channel is set up once, it is possible for these two parties to conduct an unlimited amount of transactions without ever touching the information stored on the blockchain

(4) With each transaction, both parties sign an updated balance sheet in order to always reflect how much of the bitcoin stored in the multi-sig wallet belongs to whom

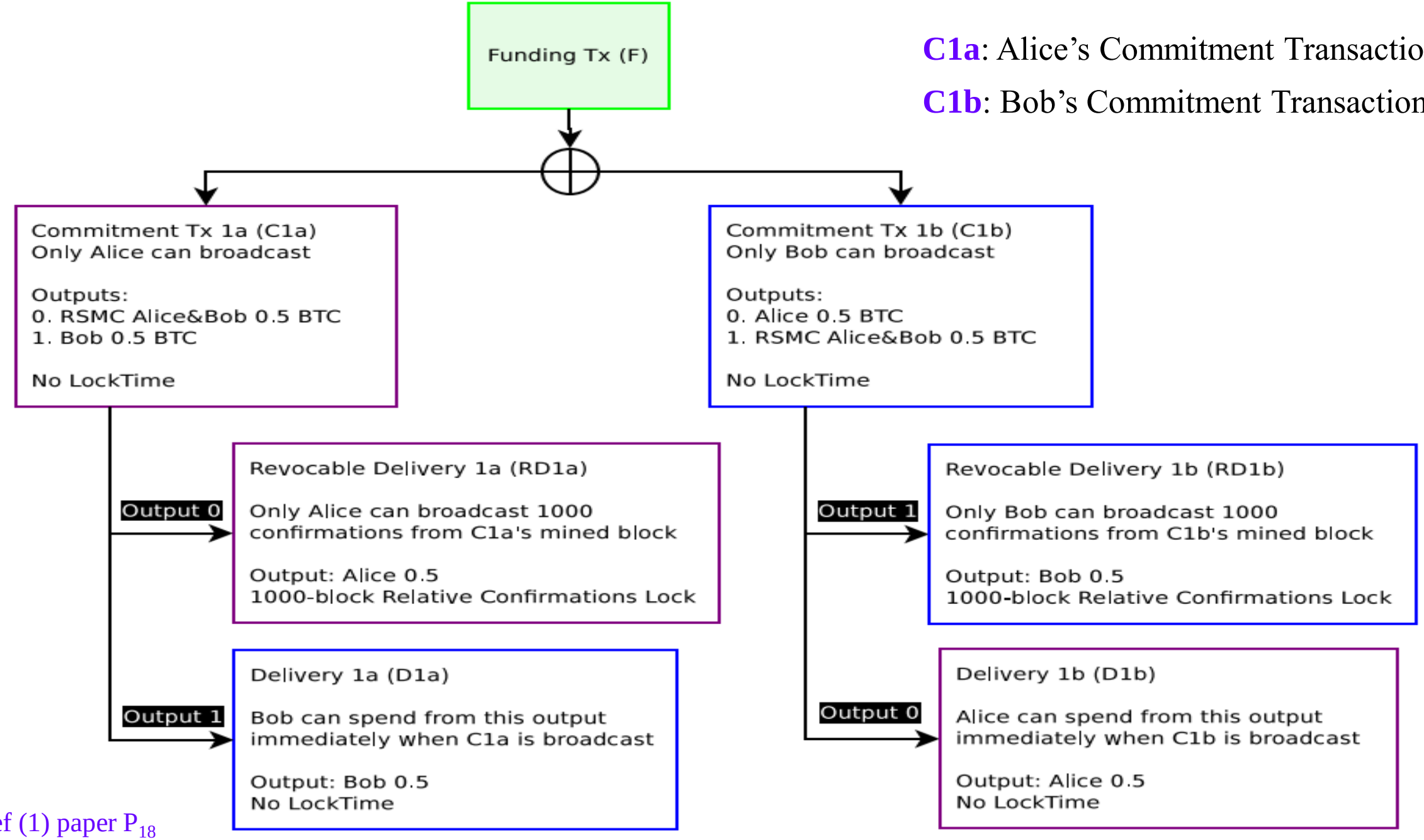
(5) The updated balance sheet is not uploaded to the blockchain but rather both parties keep a copy of it

(6) Whenever there is a dispute or the payment channel is closed, both parties can use the most recent mutually signed balance sheet to pay out their share of the multi-sig wallet

Revocable Sequence Maturity Contract (RSMC)

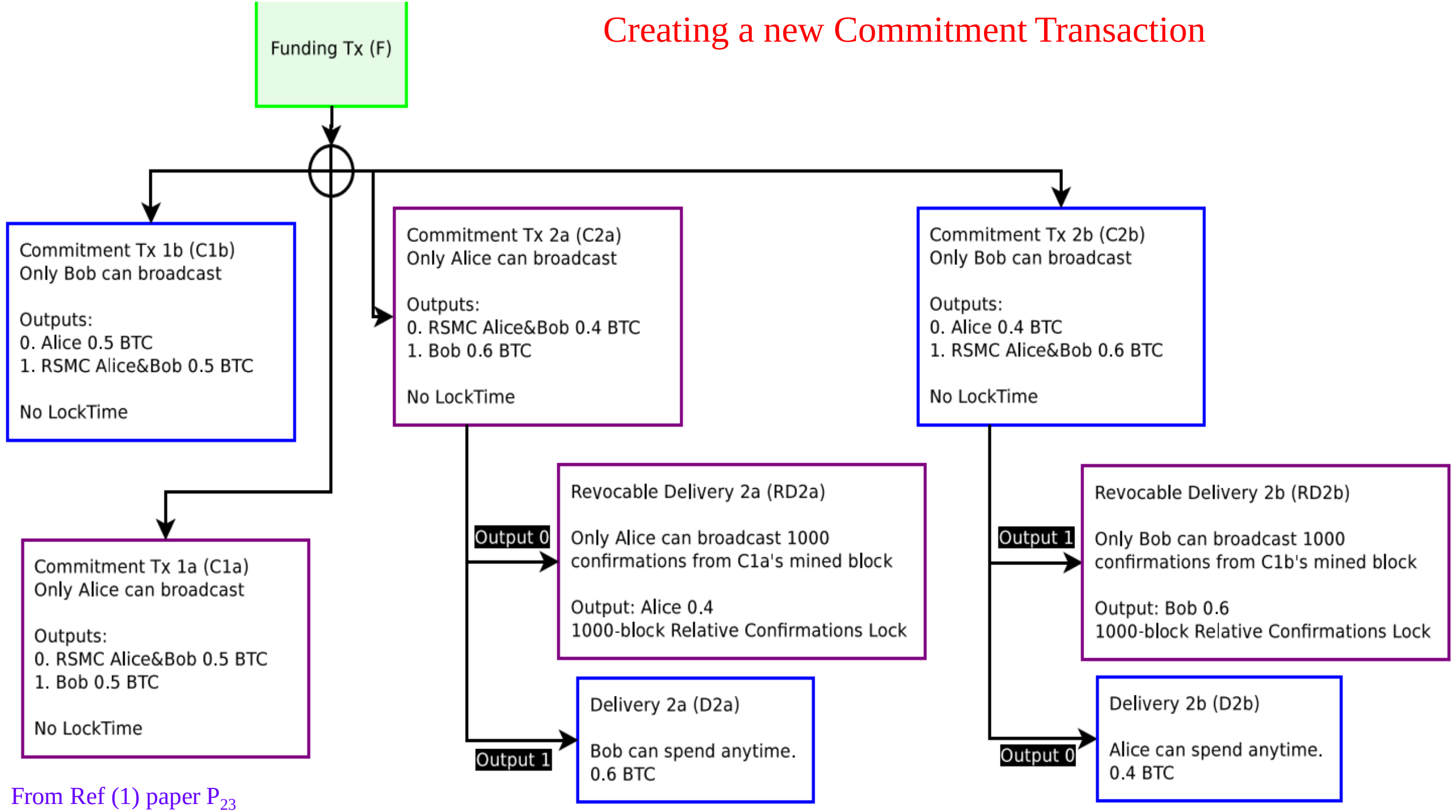
C1a: Alice's Commitment Transaction

C1b: Bob's Commitment Transaction



From Ref (1) paper P_{18}

Creating a new Commitment Transaction



From Ref (1) paper P_{23}

Revoking Prior Commitments (one party breaches contract)

(C1a/C1b) ⟶ (C2a/C2b)

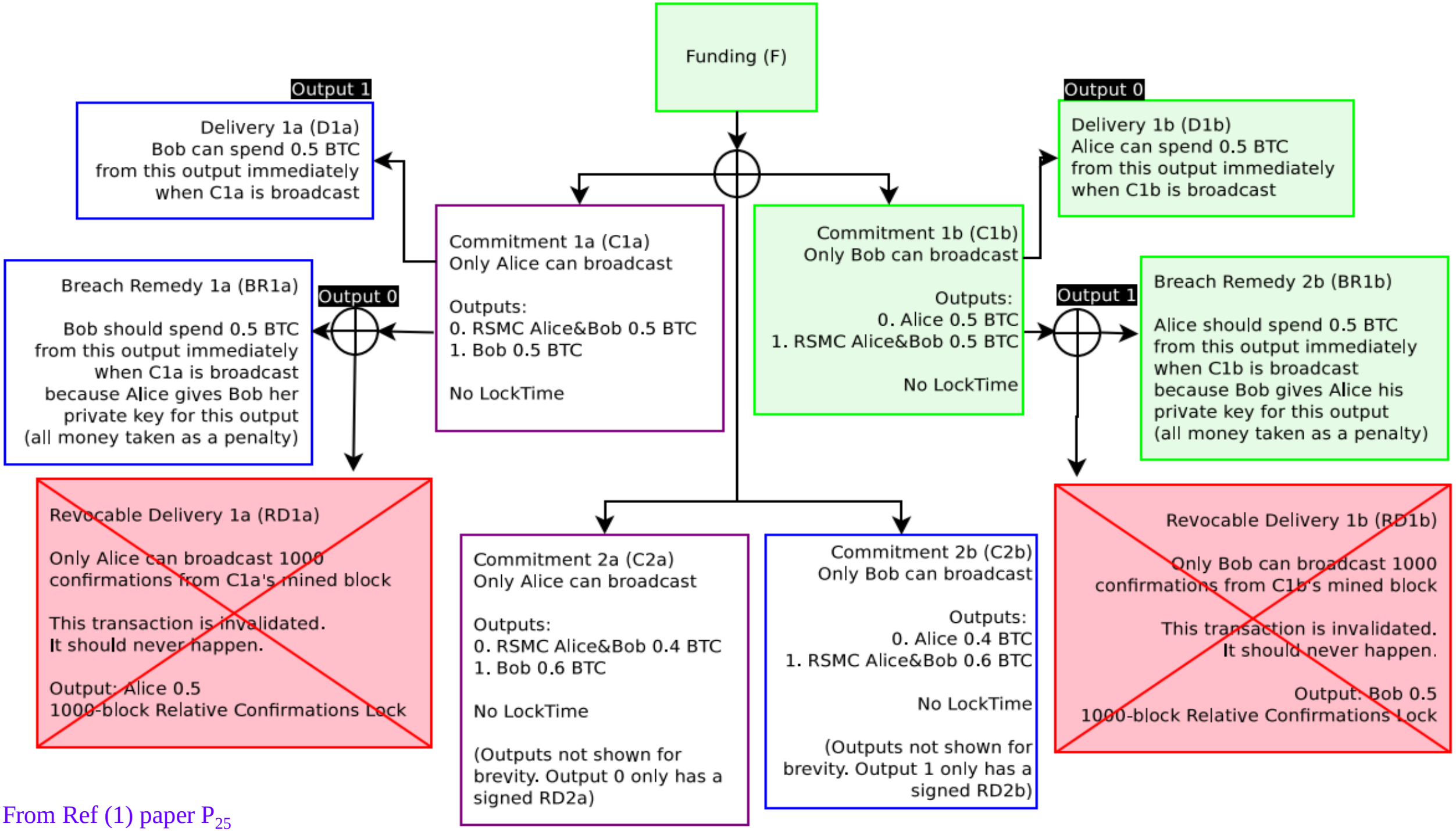
Invalidate old Commitment Transaction (C1a/C1b)

Alice and Bob both sign a Breach Remedy Transaction

If Bob broadcasts C1b, so long as Alice watches the blockchain within the predefined number of blocks (in this case, 1000 blocks), Alice will be able to take all the money in this channel by broadcasting RD1b.

However, if Alice does not broadcast BR1b within 1000 blocks, Bob's Revocable Delivery Transaction (RD1b) becomes valid after 1000 blocks.

According to Bitcoin blockchain consensus, the time for dispute has ended.



From Ref (1) paper P_{25}

Revoking Prior Commitments (both parties follow contract)

Method 1:

To invalidate C1a and C1b, both parties exchange Breach Remedy Transaction (BR1a/BR1b) signatures for the prior commitment C1a/C1b.

Alice sends BR1a to Bob using $K_{AliceRSMC1}$, and Bob sends BR1b to Alice using $K_{BobRSMC1}$.

The channel state is now at Commitment C2a/C2b and the balances are now committed.

Method 2:

Just disclosing the private keys to the counterparty.

If Bob wishes to invalidate C1b, he sends his private keys used in C1b to Alice (he does NOT disclose his keys used in C1a, as that would permit coin theft)

Cooperatively Closing Out a Channel

When either party wishes to close out a channel cooperatively, they will be able to do so by contacting the other party and spending from the Funding Transaction with an output of the most current Commitment Transaction directly with no script encumbering conditions. No further payments may occur in the channel.

both parties will be able to receive their funds immediately (instead of one party waiting for the Revocation Delivery transaction to become valid).

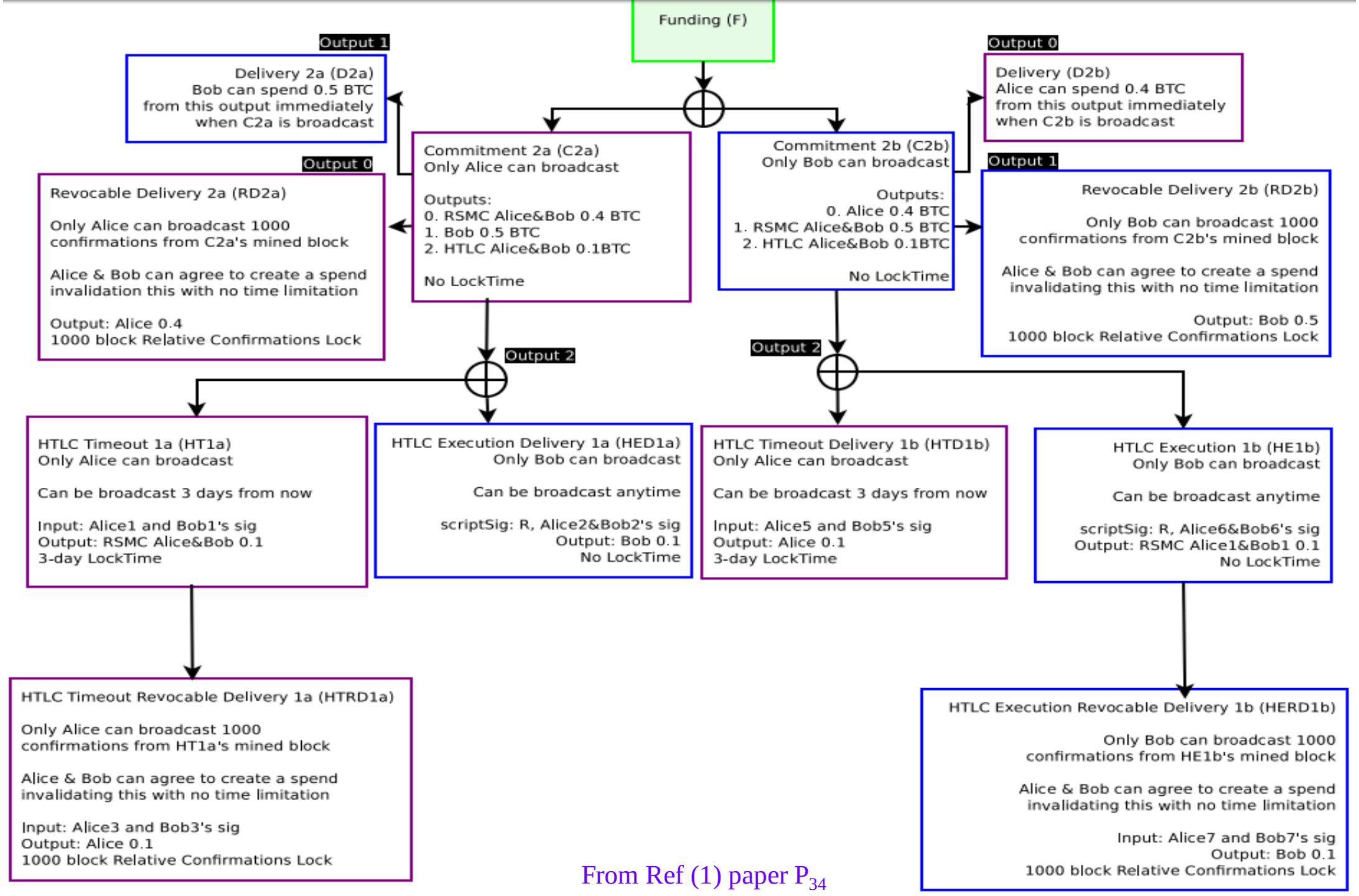
Hashed Timelock Contract (HTLC) P_{30}

HTLC is to allow for global state across multiple nodes via hashes. This global state is ensured by time commitments via disclosure of preimages R.

1. If Bob knows 20-byte random input data R from a known hash H, within three days, then Alice will settle the contract by paying Bob 0.1 BTC.

2. If three days have elapsed, the above clause is null and void, the funds are refunded back to the sender Alice.

3. Violation of the above terms will incur a maximum penalty of the funds locked up in this contract, to be paid to the non-violating counterparty as a fidelity bond.



From Ref (1) paper P_{34}

HTLC Off-chain Termination P_{37}

If the recipient can prove knowledge of R to the counterparty, the recipient is proving that they are able to immediately close out the channel on Bitcoin blockchain and receive funds.

If both parties wish to keep the channel open, they should terminate the HTLC off-chain and create a new Commitment Transaction reflecting the new balance.

If the recipient is not able to prove knowledge of R by disclosing R, both parties should agree to terminate the HTLC and create a new Commitment Transaction with the balance in the HTLC refunded to the sender.

If they are terminating a particular HTLC, they should also exchange some of their own private keys used in the HTLC transactions.

Seeing the picture from Ref (1) paper P39.

Decrementing Timelocks---over a multi-hop payment network P_{44}

Presume Alice wishes to send 0.001 BTC to Dave.

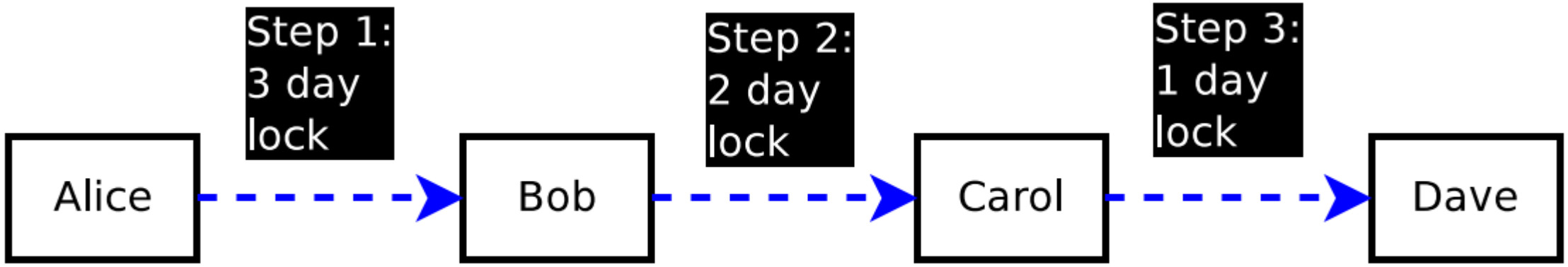


Figure 15: Payment over the Lightning Network using HTLCs.

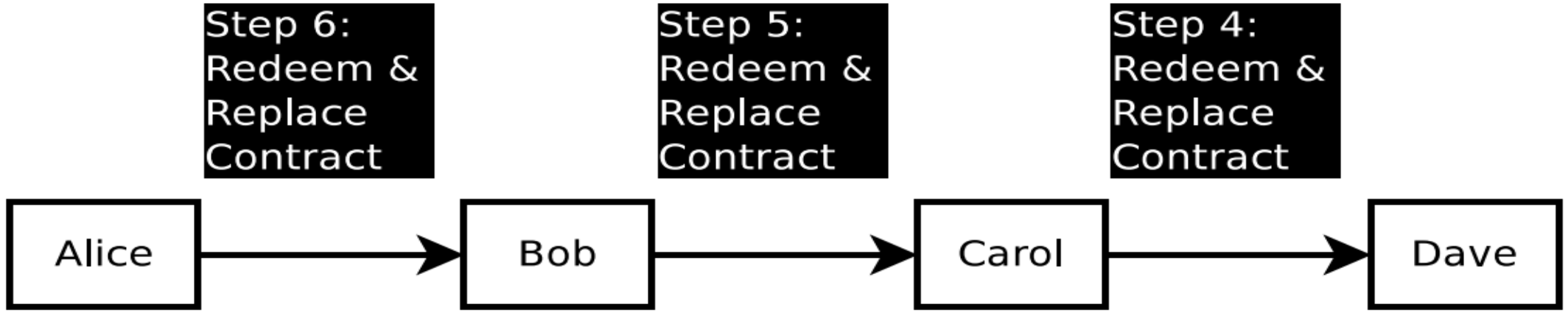
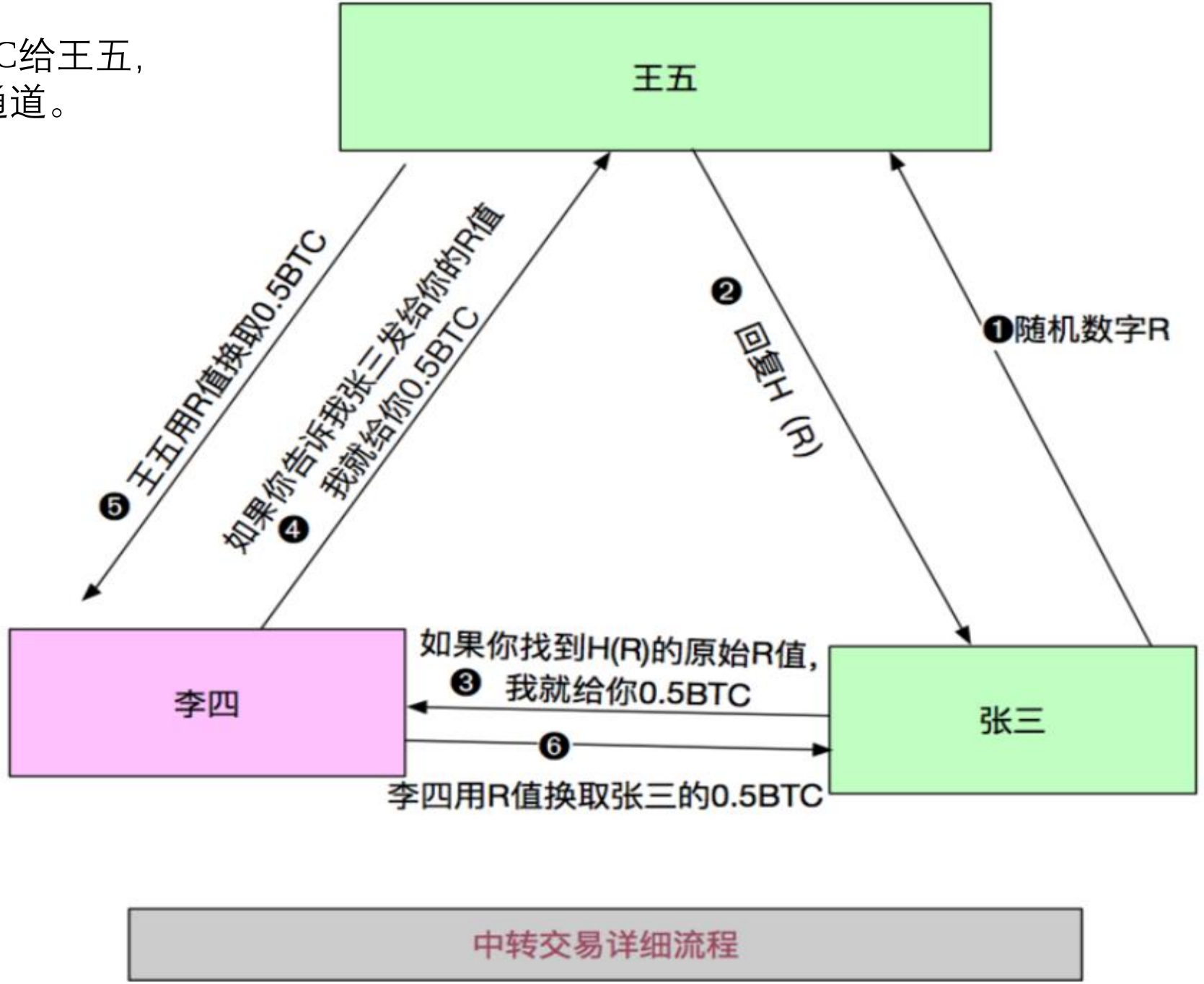


Figure 16: Settlement of HTLC, Alice's funds get sent to Dave.

张三想支付0.5BTC给王五，
但两人没有交易通道。



中转交易详细流程

Ref. https://www.jianshu.com/p/e326802294e1

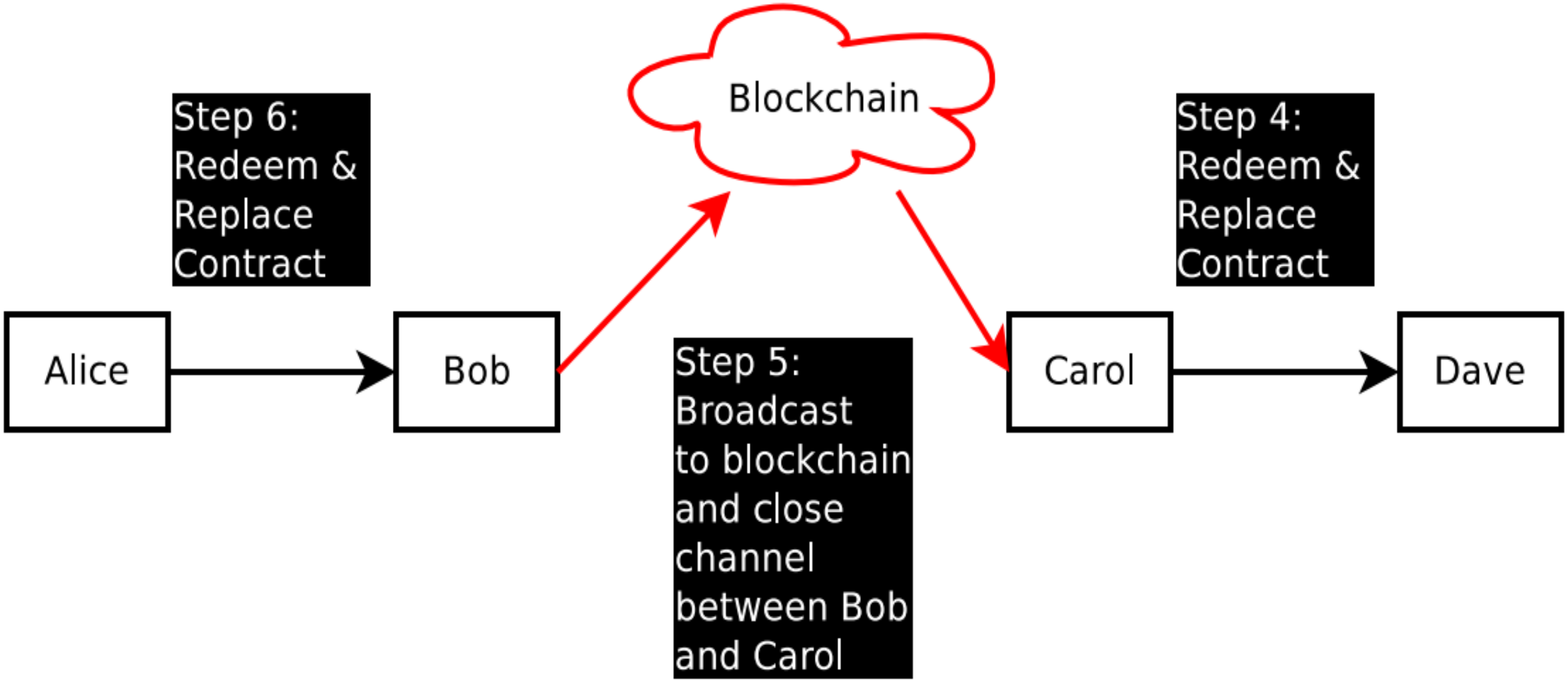


Figure 17: Only the non-responsive channels get broadcast on the blockchain, all others are settled off-chain via novation.

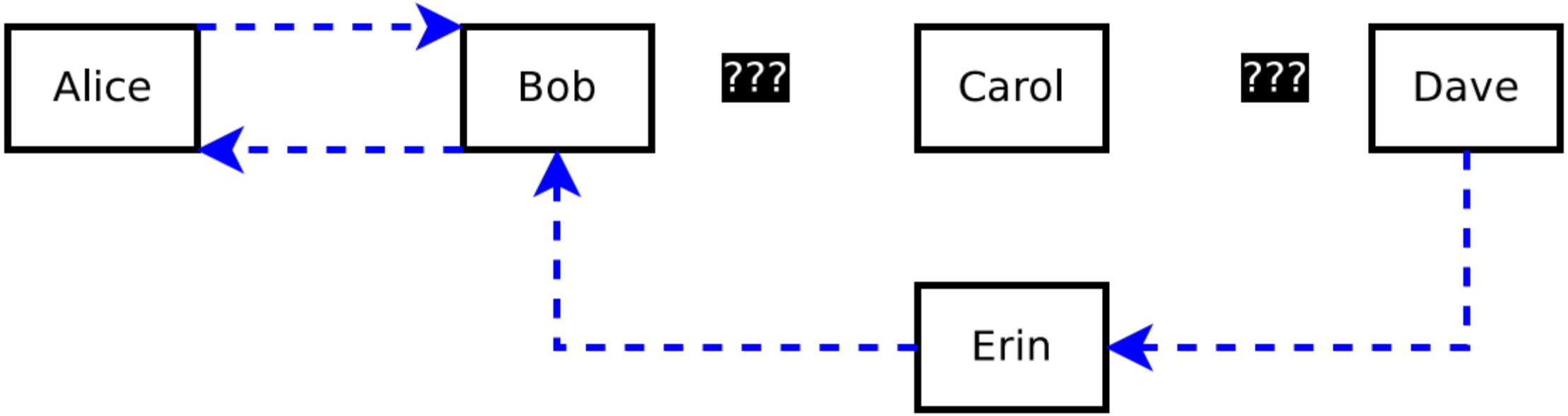
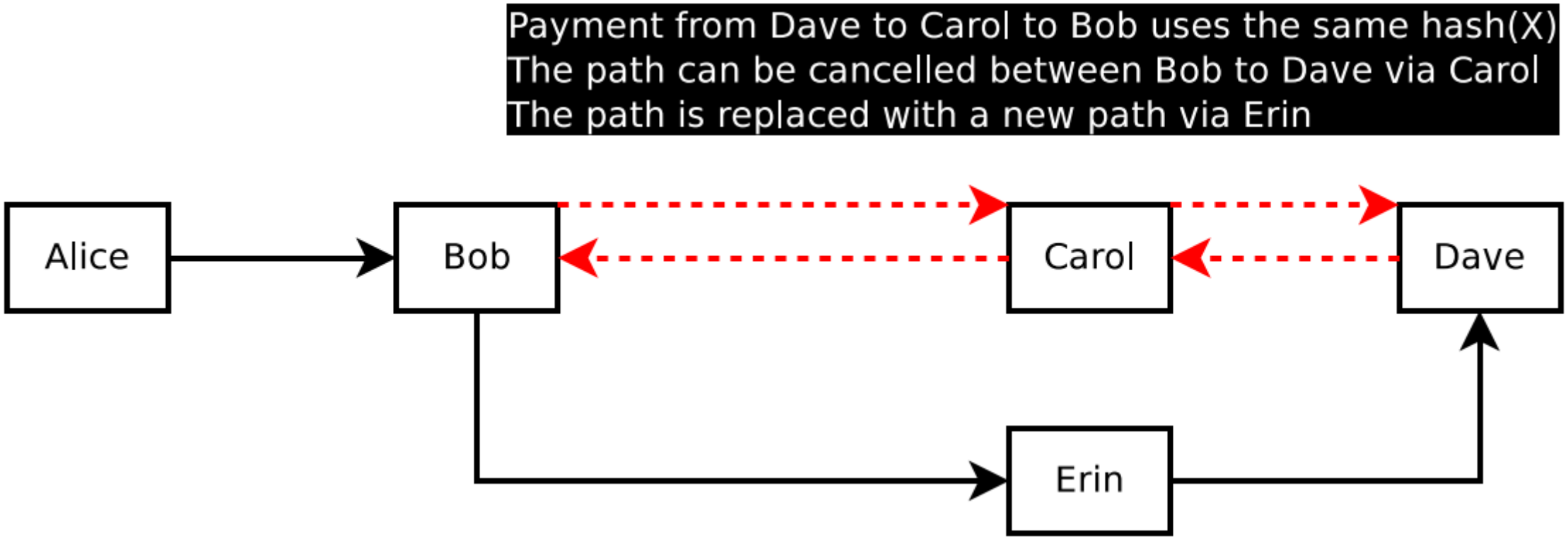


Figure 18: Dave creates a path back to Alice after Alice fails to send funds to Dave, because Carol is uncooperative. The input R from hash(R) is never brodcast by Dave, because Carol did not complete her actions. If R was broadcast, Alice will break-even. Dave, who controls R should never broadcast R because he may not receive funds from Carol, he should let the contracts expire. Alice and Bob have the option to net out and close the contract early, as well, in this diagram.

A new path from Alice to Dave



Reference

Poon J, Dryja T. The bitcoin lightning network: Scalable off-chain instant payments[J]. See https://lightning. network/lightning-network-paper. pdf, 2016.
https://lightning.network/lightning-network-paper.pdf

https://www.bilibili.com/video/av18042505/

https://www.jianshu.com/p/e326802294e1

https://medium.com/@argongroup/bitcoin-lightning-network-7-things-you-should-know-604ef687af5a