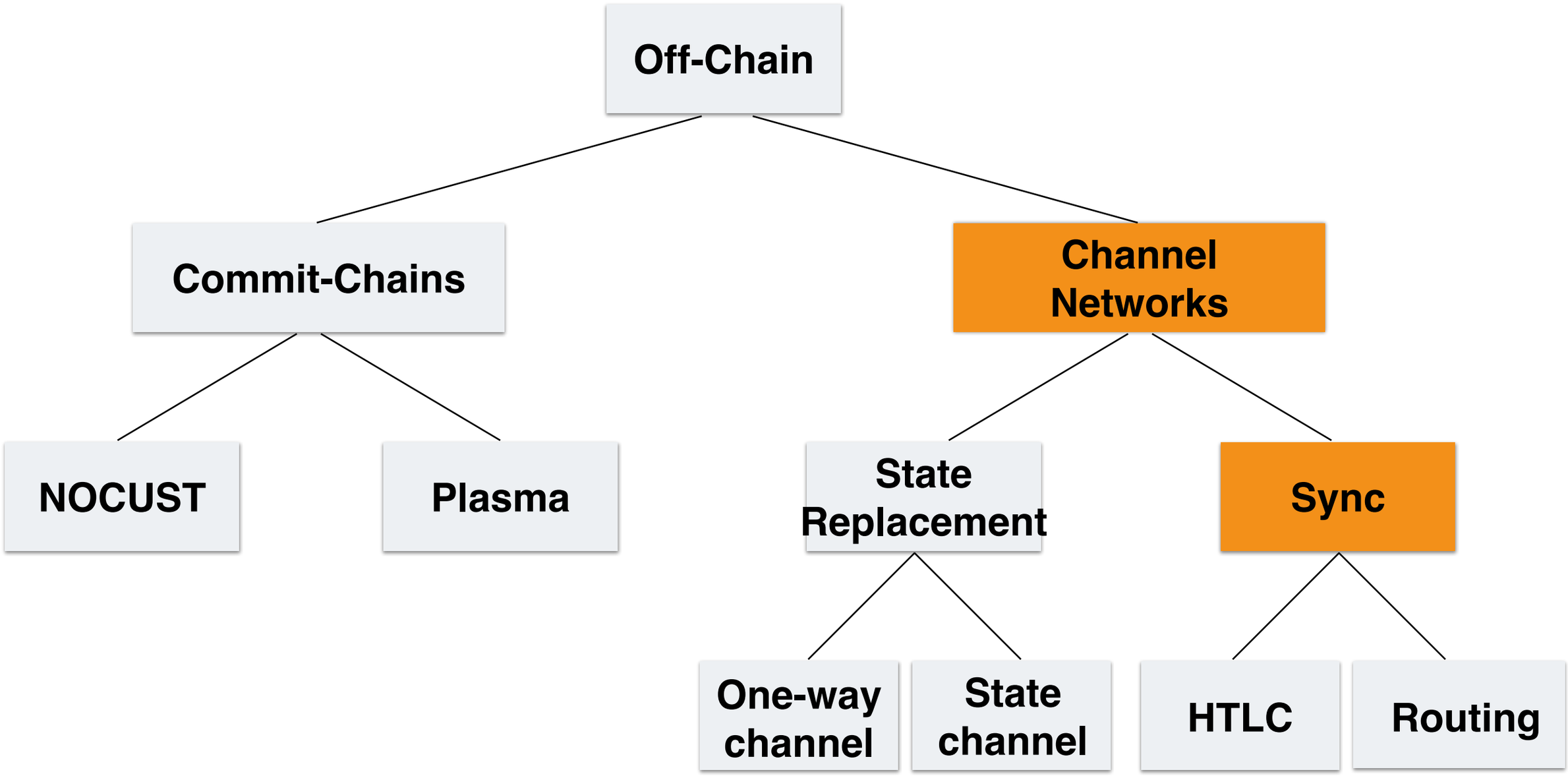
Channel Networks
HTLC

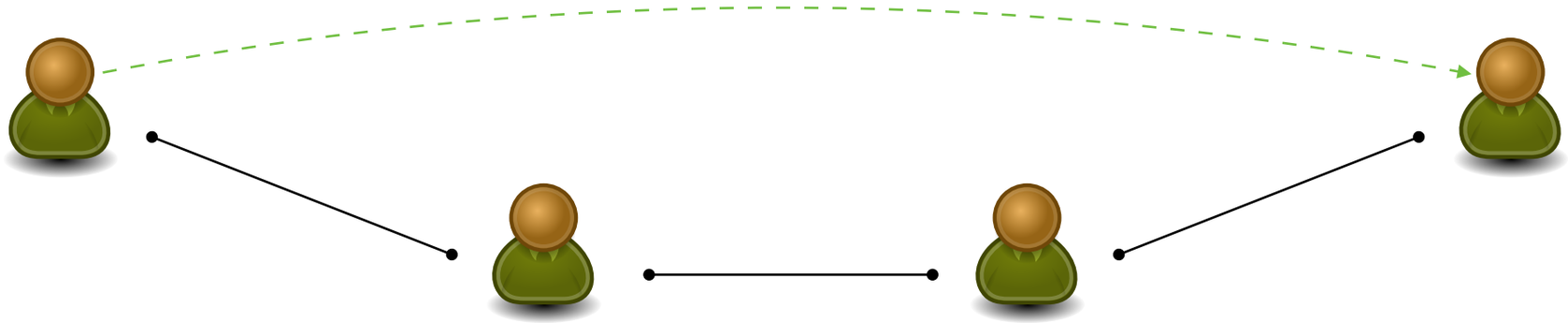
Which Off-Chain Solution?



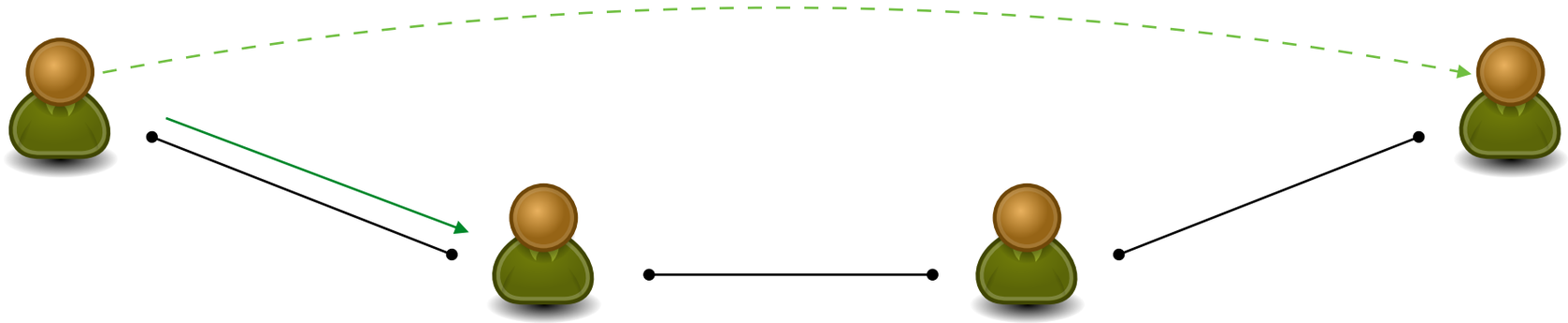
Payment Channel Network

Payment Channel Network

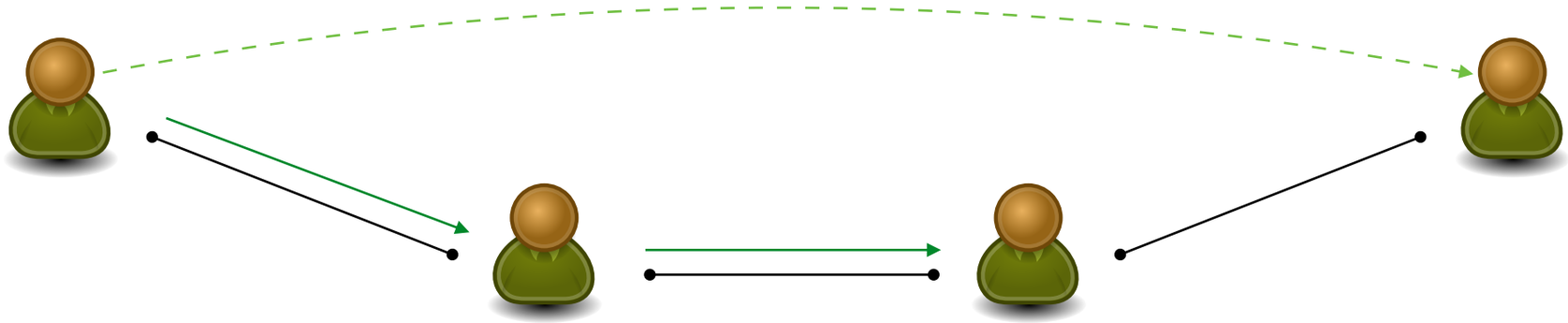
Payment Channel Network



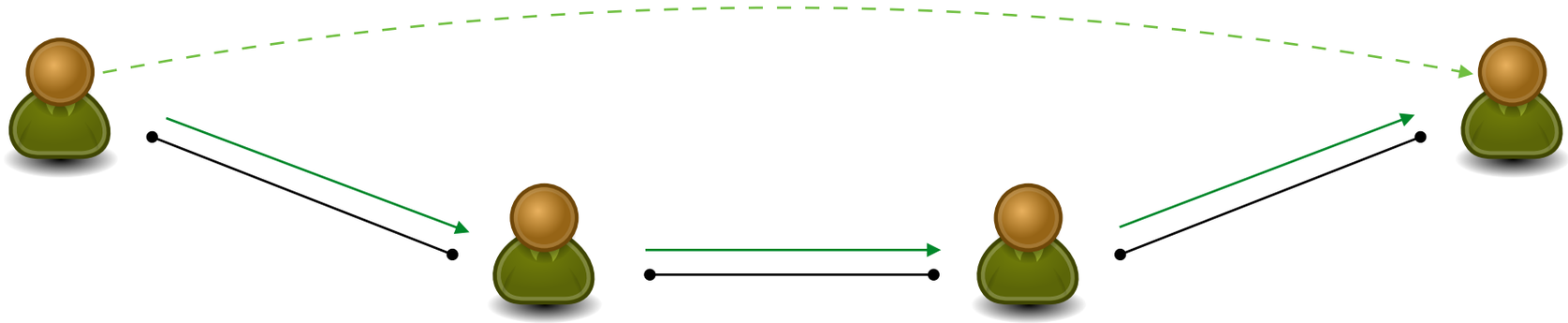
Payment Channel Network



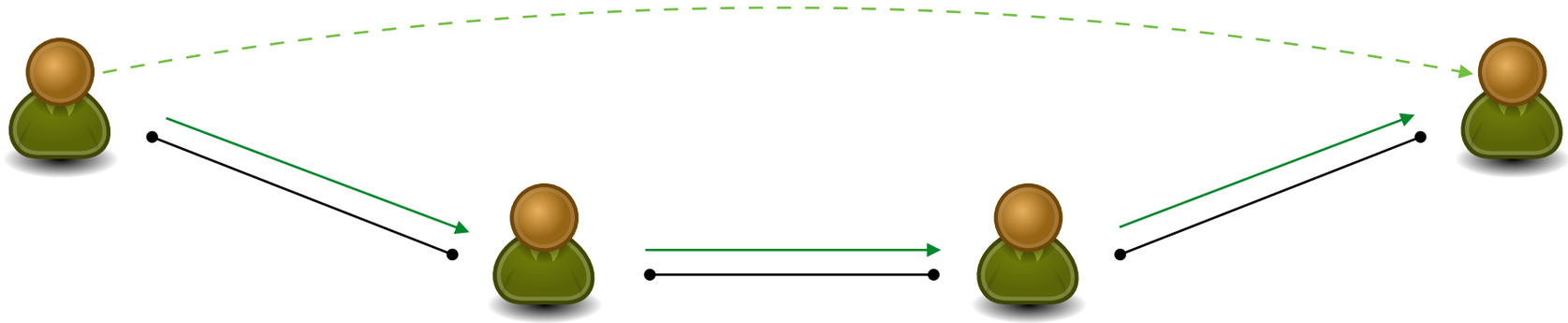
Payment Channel Network



Payment Channel Network



Payment Channel Network

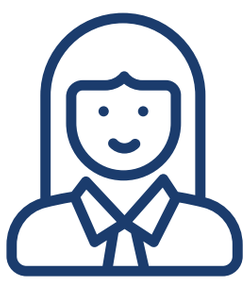


We need a **simple conditional transfer**.

A Humble Conditional Transfer

A Humble Conditional Transfer

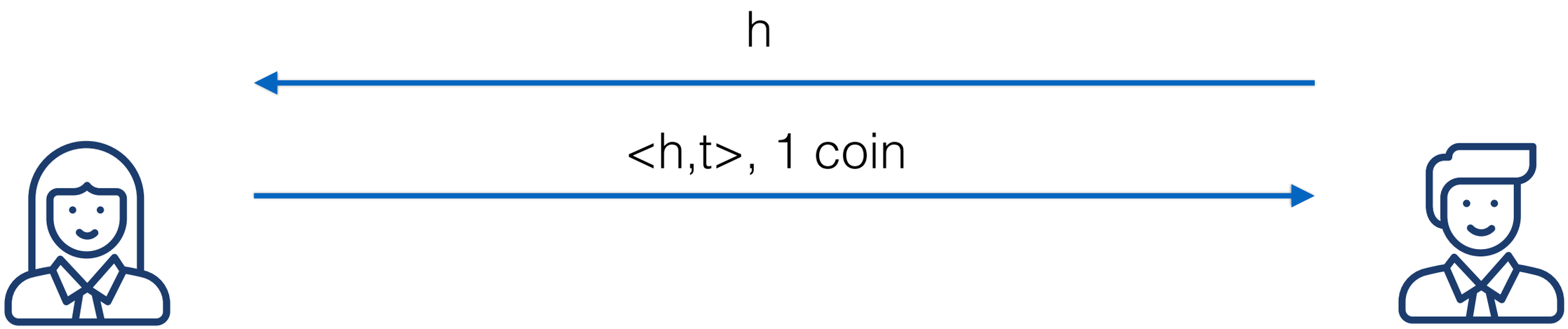
h



h = H(R)

(1) Jackson computes H(R) and shares h

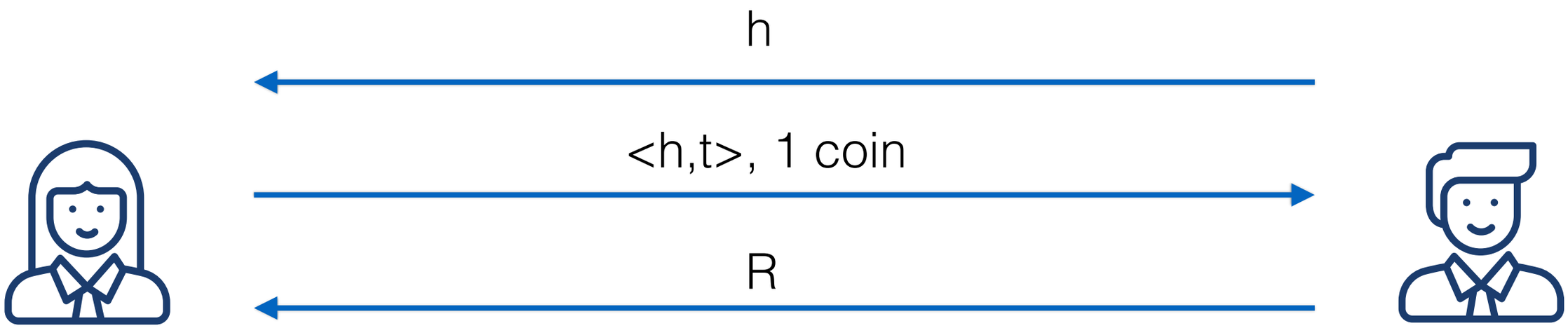
A Humble Conditional Transfer



(1) Jackson computes H(R) and shares h

(2) Michaela's conditional transfer: *"Jackson, if you reveal R before time t, you get the coins"*

A Humble Conditional Transfer

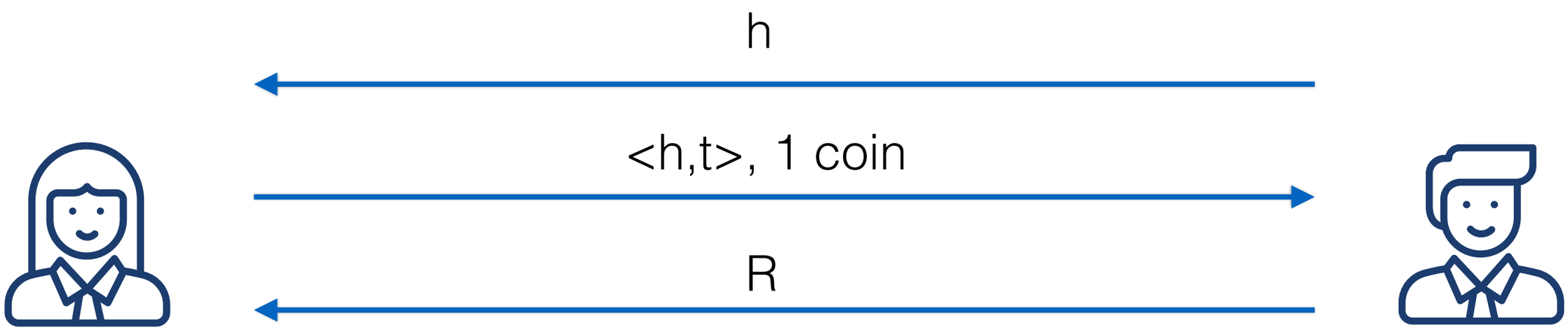


(1) Jackson computes H(R) and shares h

(2) Michaela's conditional transfer: *"Jackson, if you reveal R before time t, you get the coins"*

(3) Jackson reveals R

A Humble Conditional Transfer



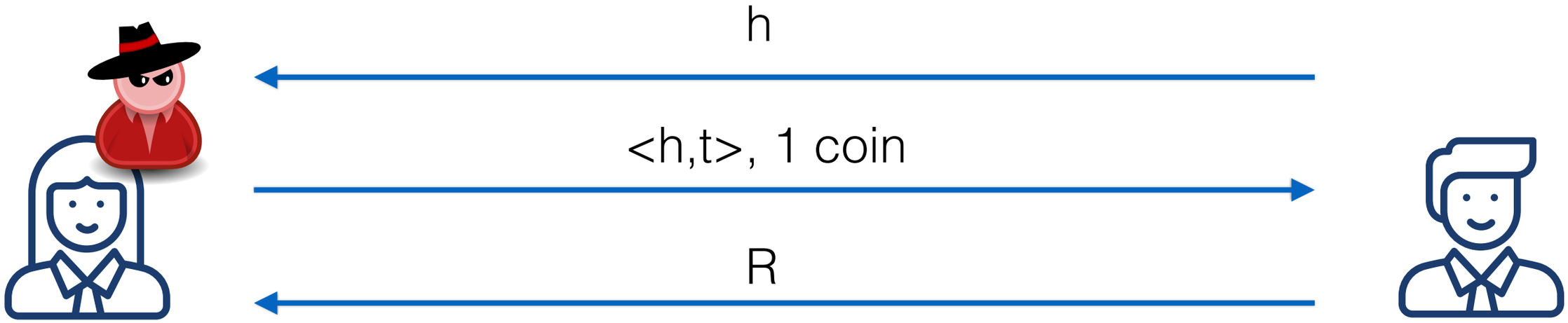
(1) Jackson computes H(R) and shares h

(2) Michaela's conditional transfer: *"Jackson, if you reveal R before time t, you get the coins"*

(3) Jackson reveals R

(4) Michaela cooperates

A Humble Conditional Transfer



(1) Jackson computes H(R) and shares h

(2) Michaela's conditional transfer: *"Jackson, if you reveal R before time t, you get the coins"*

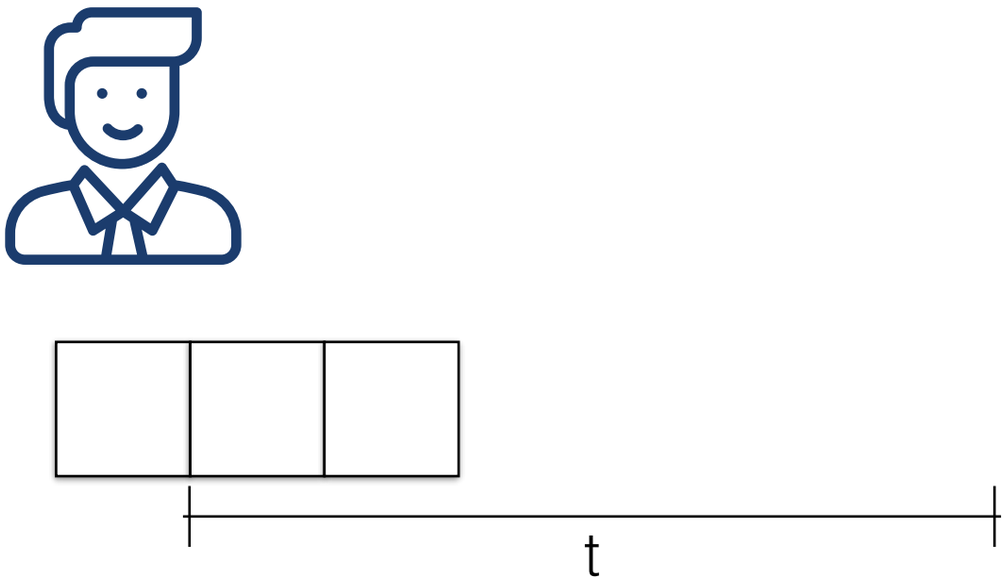
(3) Jackson reveals R

(4) Michaela cooperates

..what if Michaela doesn't cooperate?

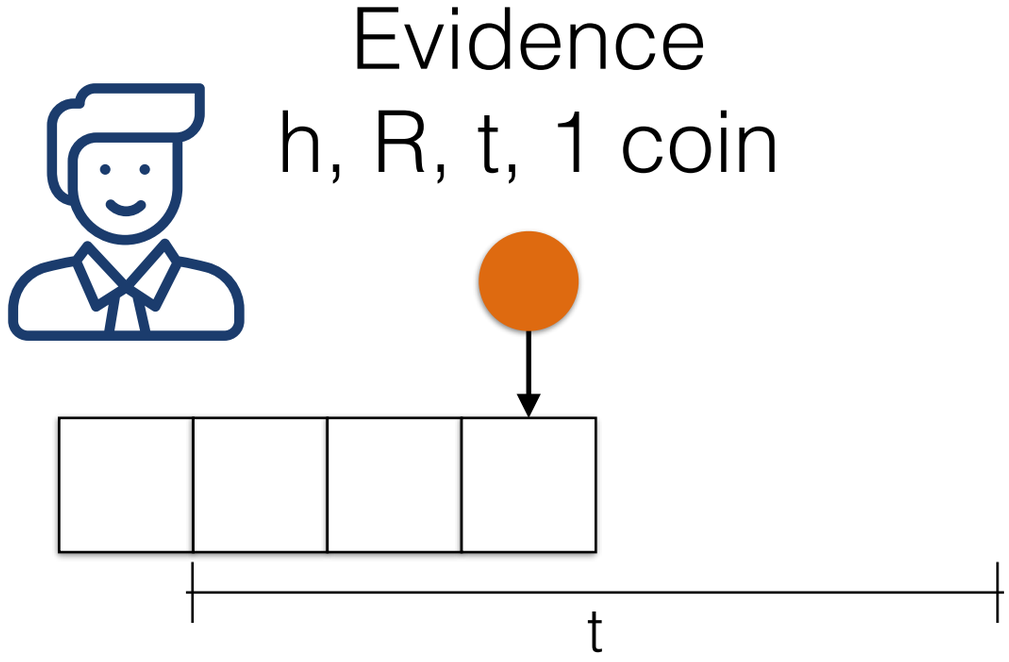
Hashed Time-locked Contract

== conditional transfer + evidence



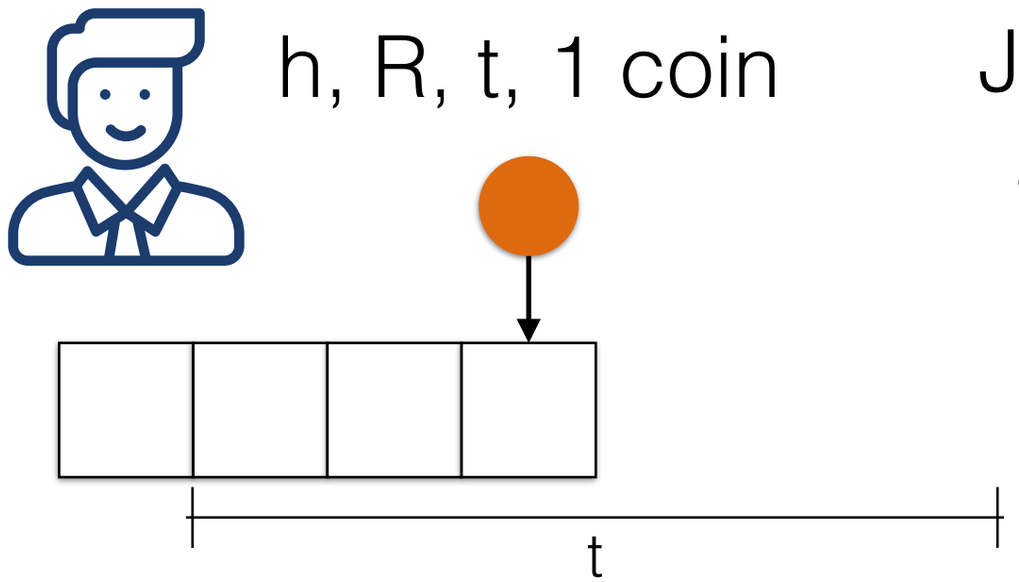
Hashed Time-locked Contract

== conditional transfer + evidence



Hashed Time-locked Contract

== conditional transfer + evidence

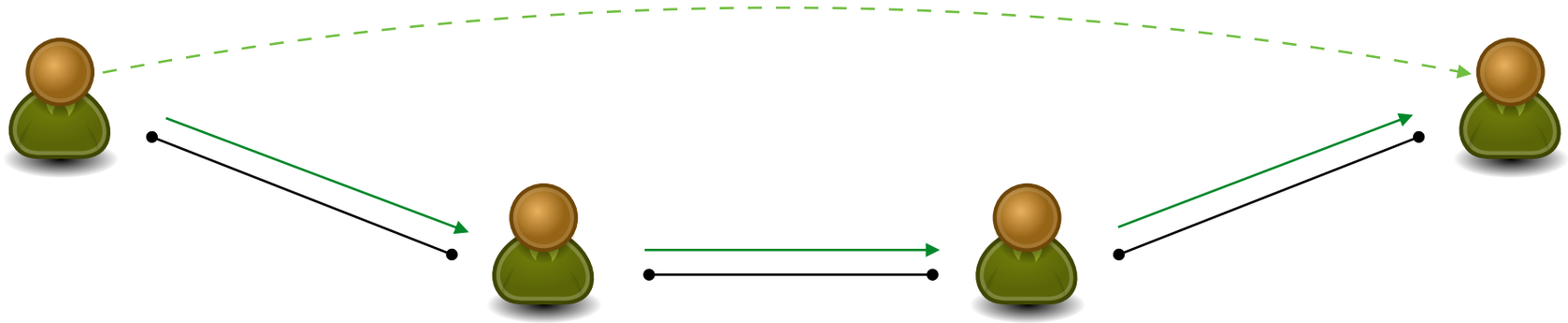


Evidence
h, R, t, 1 coin

The blockchain confirms that Jackson revealed R before time t and complied with the contract

-> He receives the coin.

Payment Channel Networks



Path-based Payments (HTLC)

We can synchronise a payment among peers on the path!

Path-based virtual Payment Channels (Perun)

We can set up a virtual channel to avoid intermediary peers to be responsive!