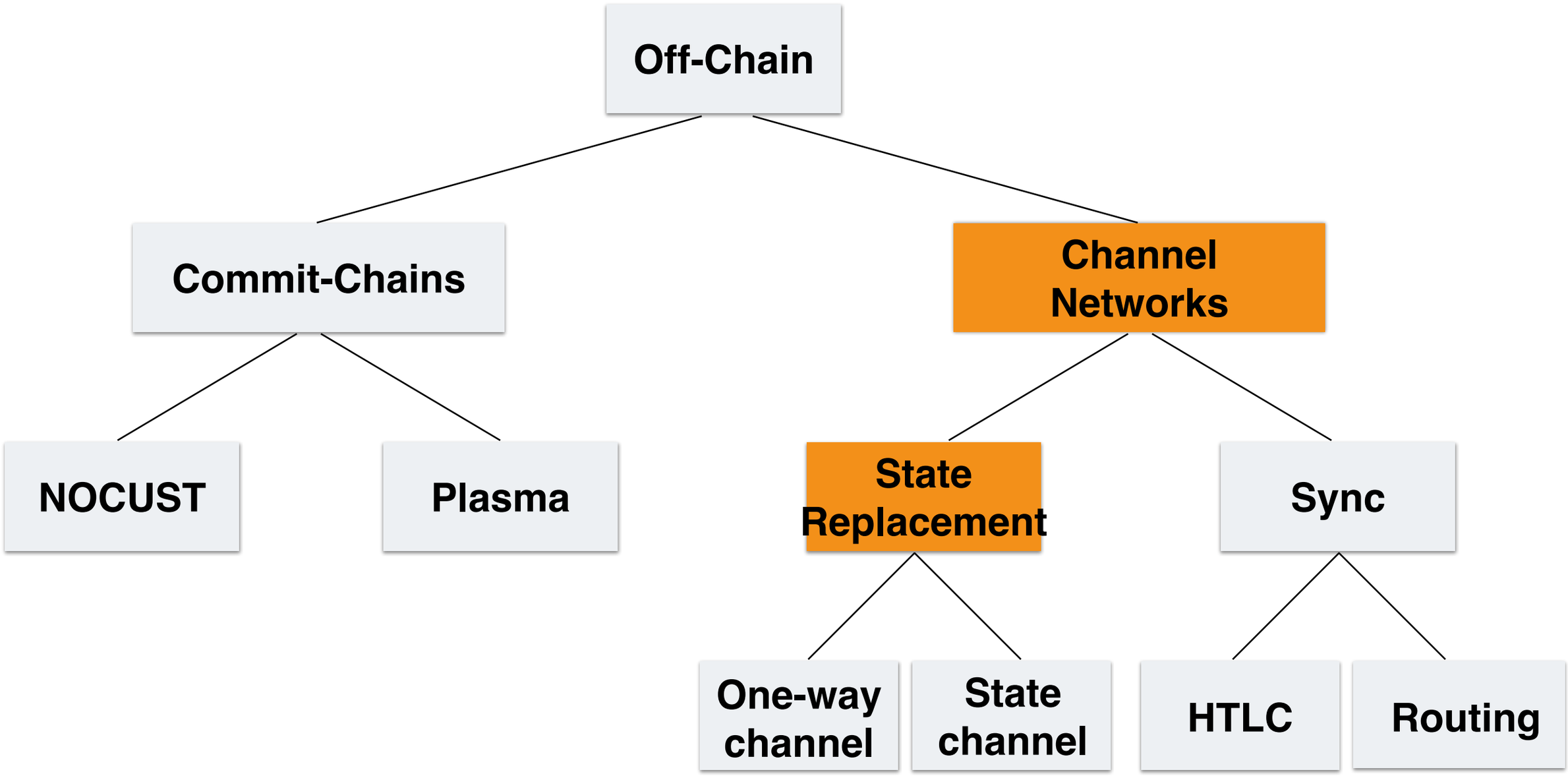
Channel Networks State Replacement

Which Off-Chain Solution?



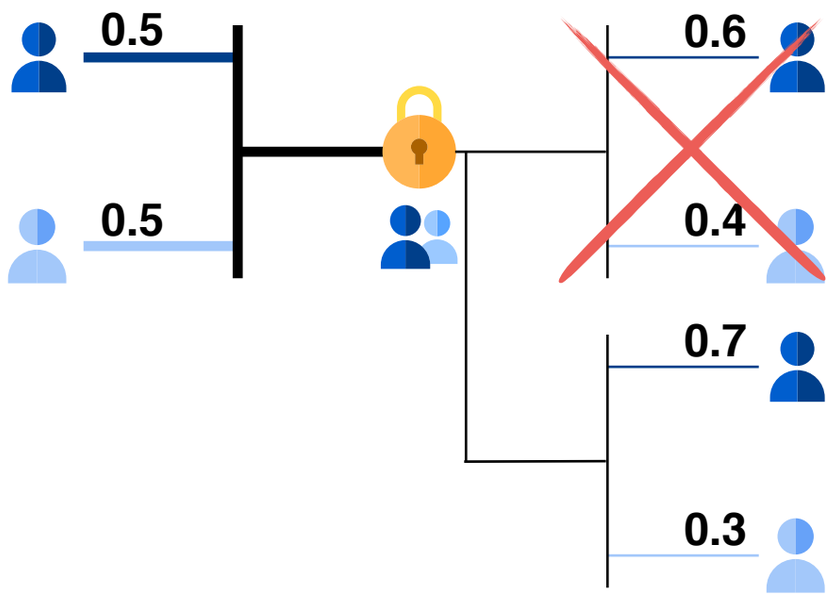
Payment Channel (redistribution of assets)

Spilman	Duplex Micropayment	Lightning

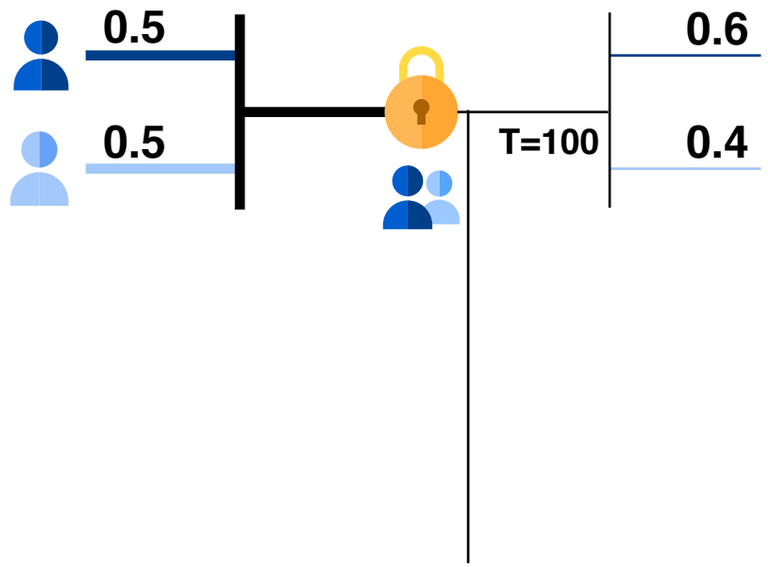
State Channel (game, voting, auctions, etc)

Sprites	Perun	Kitsune

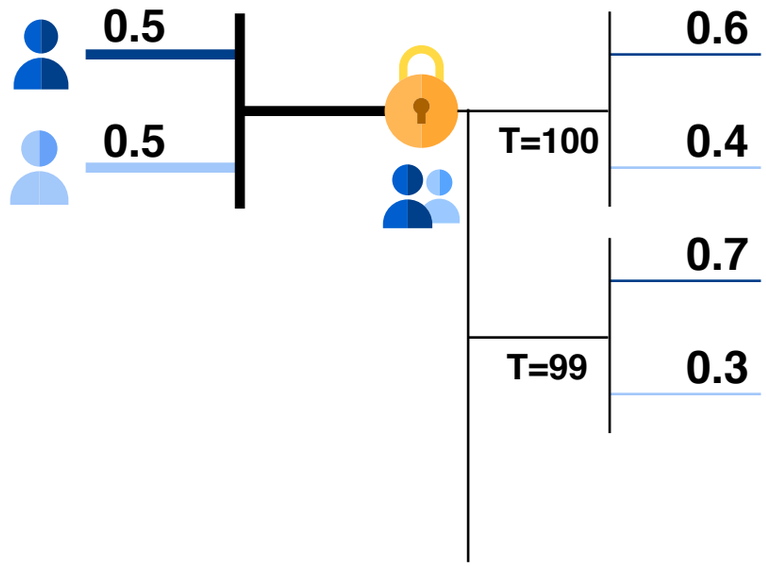
State Replacement



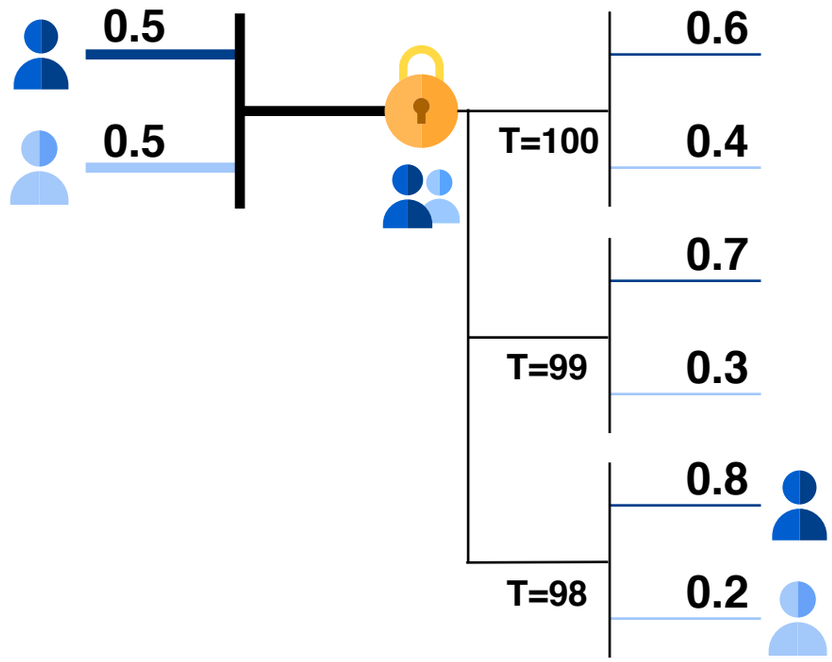
Time Lock State Replacement



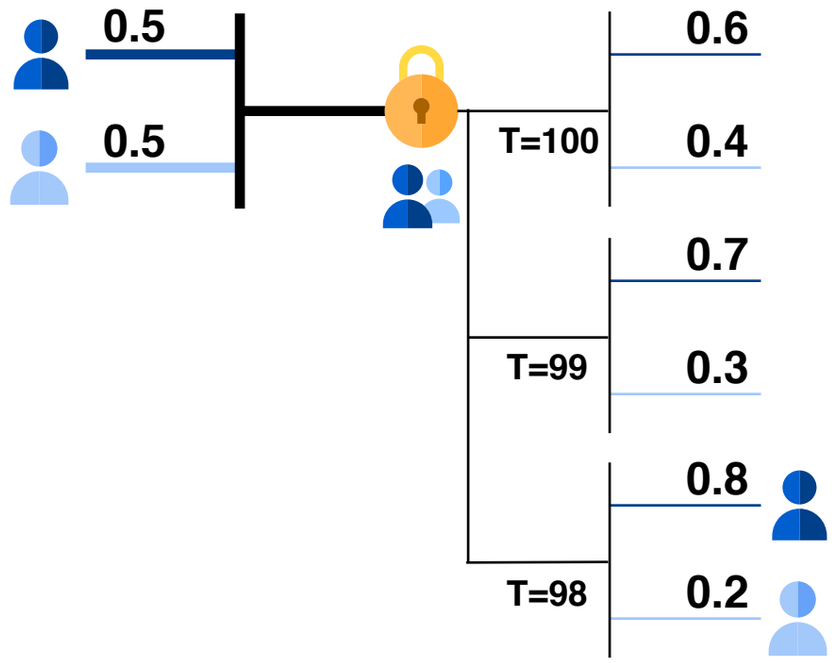
Time Lock State Replacement



Time Lock State Replacement

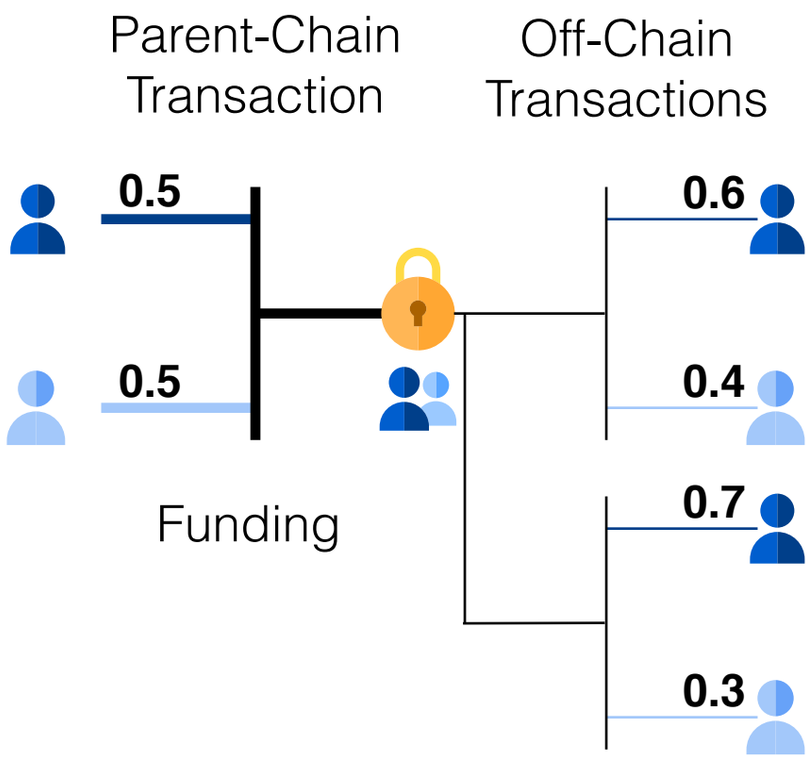


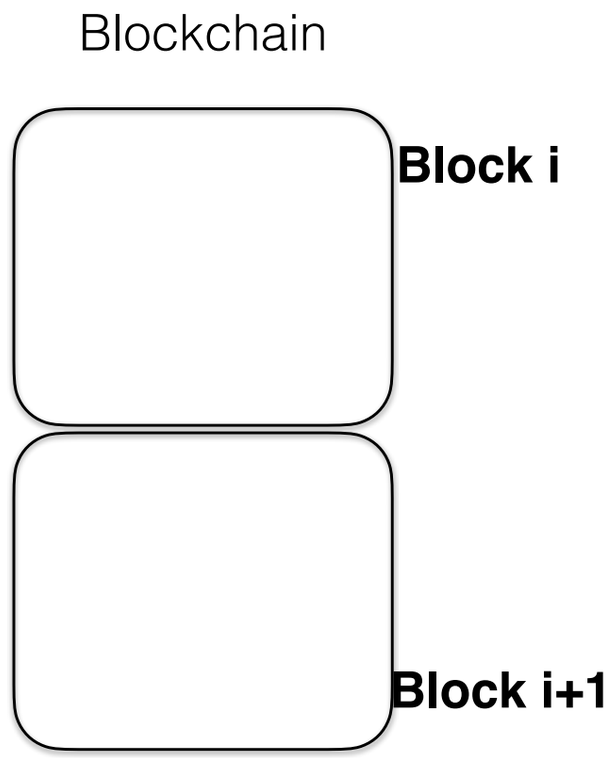
Time Lock State Replacement



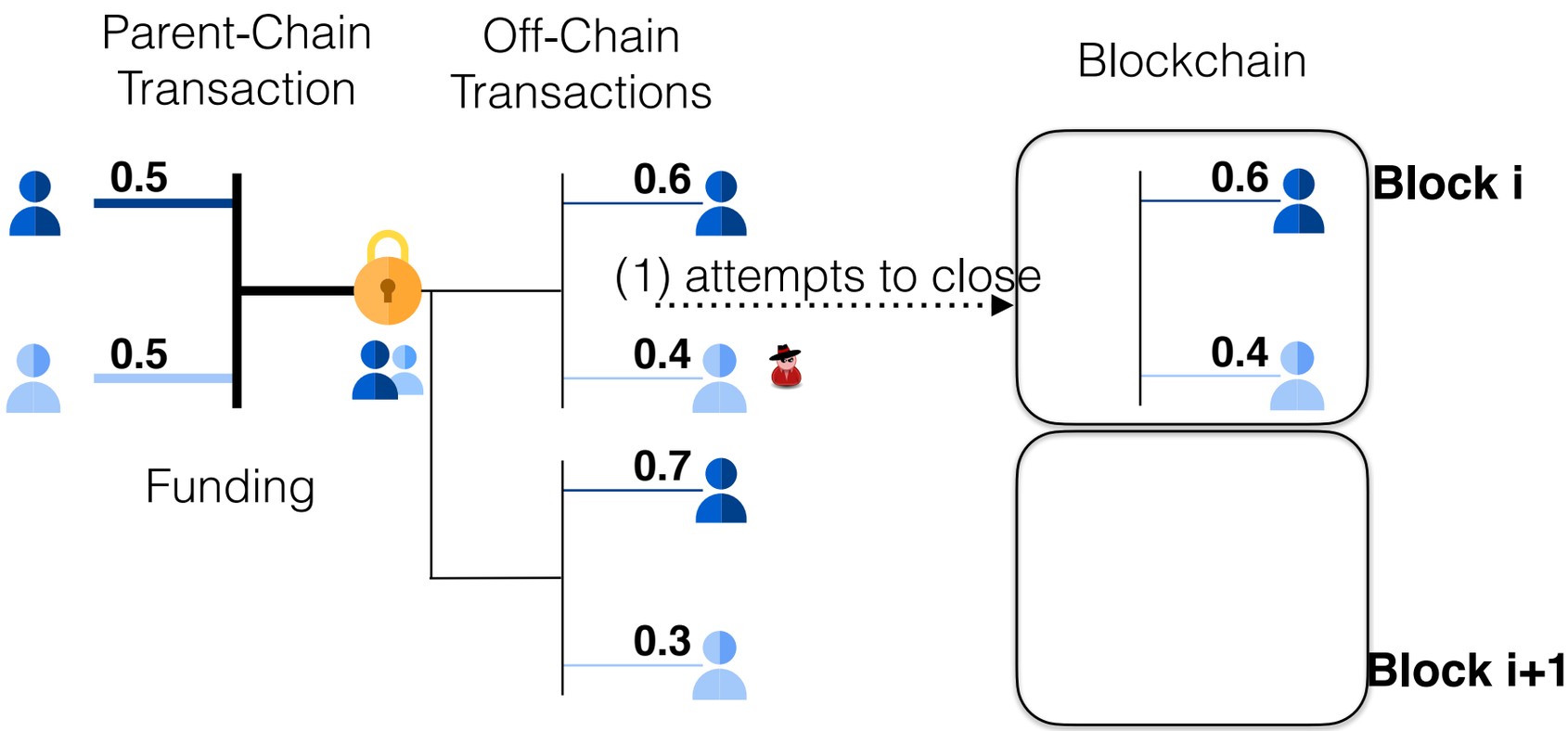
Lowest timelock is first included in the blockchain.

Revocation State Replacement (Lightning)

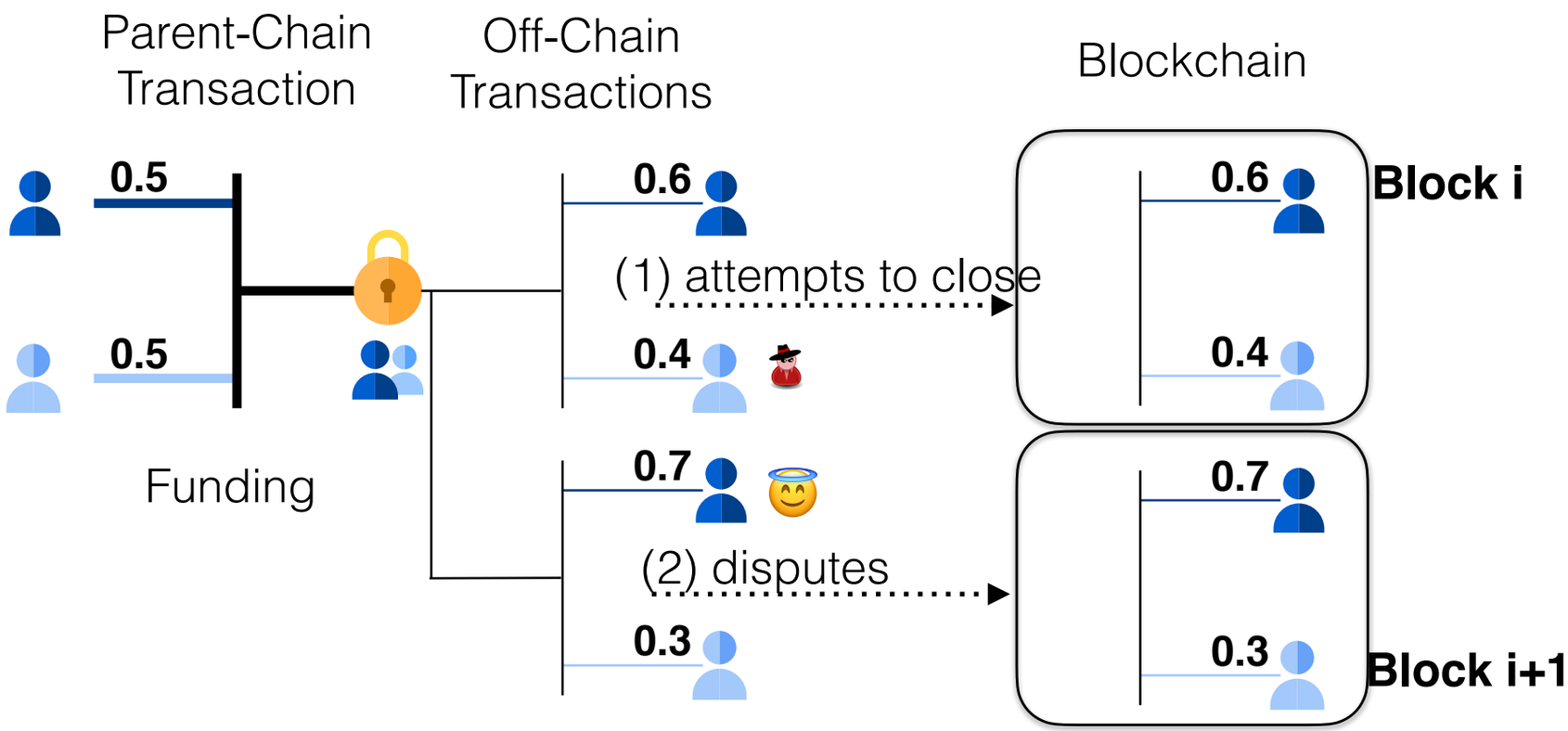




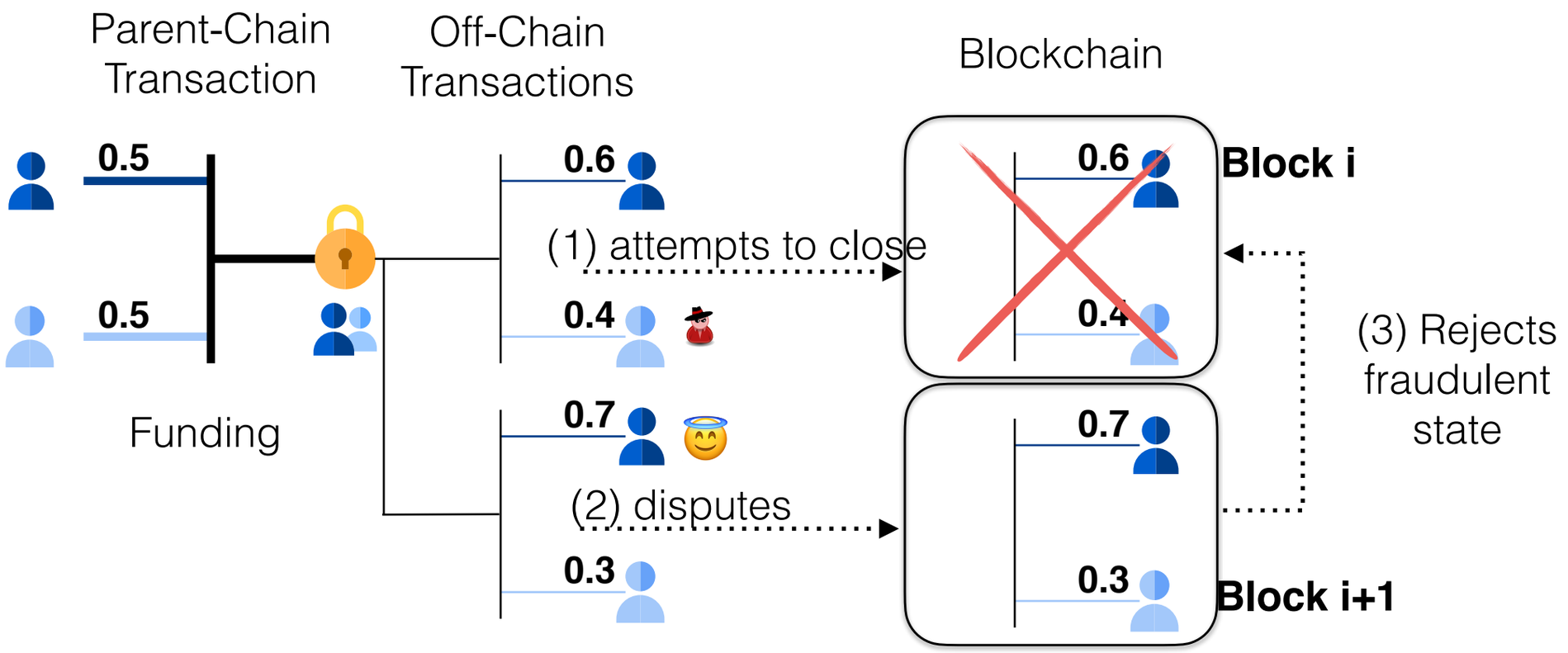
Revocation State Replacement (Lightning)



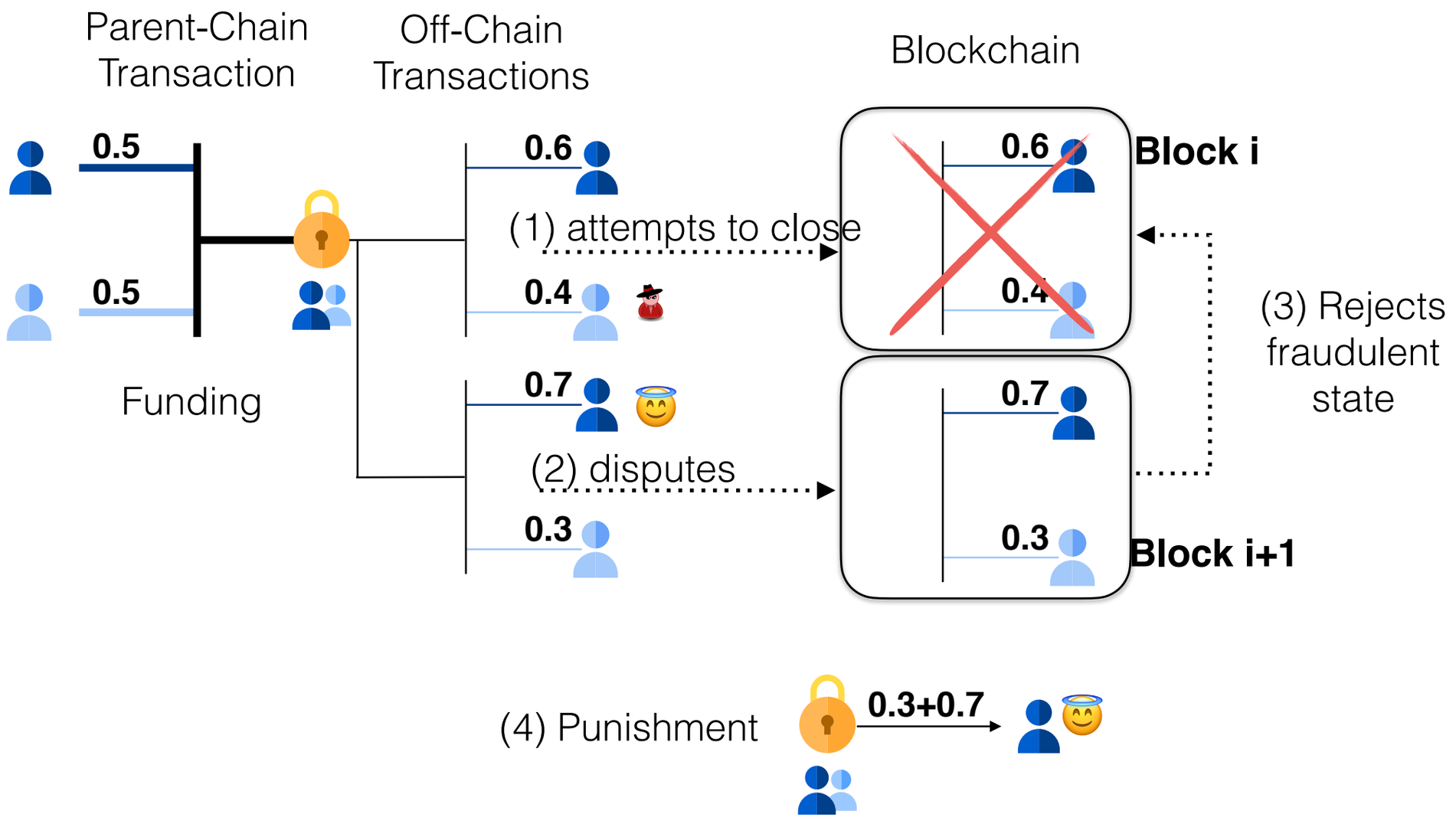
Revocation State Replacement (Lightning)



Revocation State Replacement (Lightning)



Revocation State Replacement (Lightning)



State Replacement Techniques (2013 - 2015)

Replace by..

Incentive → **One-way payments**

Spilman

Receiver signs and publishes final statement

Time Lock → **Bi-directional**

Duplex Micropayment Channels

Tension between throughput and on-chain costs
Expiry time (later removed)

Revocation → **Bi-directional, no expiry**

Lightning

Agree on last state, keep all previous revoked states

Protocol Complexity

Bitcoin's model makes it challenging to remove expiry time and throughput limitations

State Replacement Techniques (2016+)

Replace by..

Version ⟶ **State change, everyone signs**

Increment version

Sig(A), Sig(B), Hash of State(i), i