He-HTLC: Revisiting Incentives in HTLC
Sarisht Wadhwa (sarisht.wadhwa@duke.edu), Jannis Stöter, Fan Zhang and Kartik Nayak

What is HTLC?
1. Bob has an asset
2. Asset locked in contract on-chain
3a. Alice reveals preimage to get asset
3b. Bob gets refund after some timeout

Incentive Problems with HTLC
- Passive miners: Focused on the mempool, Confirms most profitable transactions
- Active miners: Engage in external protocols, e.g., add MEV software, open up direct channels to users, etc.

Modeling: Active and Passive Miners
- Alice reveals preimage
- Miner accepts the transaction
- Miner gets transaction fee and Bob gets $0

Problem in MAD-HTLC: Reverse Bribery
- Alice reveals preimage
- Miner bribes Bob more than collateral to reveal other hash lock
- Miner confiscates both MH-Dep, MH-Col
- Miner(s) gets $V + $C-bribe and Bob gets bribe
- Still preferred by miners and Bob

Key Ideas:
- i) Burn Deposit (Anti-RBA)
- ii) Use rationality of multiple miners (Anti-Bribery)

He-HTLC: An Incentive Compatible HTLC
- Bob adds both asset and collateral to a contract
- After timeout, instead of Bob, the asset and collateral go to He-Col contract
- If both preimages are released, then miners have chances to confiscate collateral which leads to deposit being burnt

Salient Aspects of He-HTLC
- Low collateral required from Bob.
- Even when all miners are active, security is not impacted.
- Instant return of collateral when honest successful execution.
- Lightweight and implementable with current Bitcoin OPcodes.
- Alice need not monitor the network after revealing.

He-HTLC: Revisiting Incentives in HTLC
Sarisht Wadhwa (sarisht.wadhwa@duke.edu), Jannis Stöter, Fan Zhang and Kartik Nayak

Three Variants of Reverse Bribery
- All miners, independent of winning the confiscation transaction, bribe Bob for his secret
- A miner bribes Bob for the secret only when the miner is able to create the block redeeming the deposit. Eliminates risk to miner.

Combining with original bribery attack, to remove dependency on collateral. Modify SDRBA to include both collateral and deposit.

MULTI-CHAPTER EDITION 1.0
https://eprint.iacr.org/2022/546.pdf