Poster: He-HTLC Revisiting Incentives in HTLC

Bibliographic reference to the paper

[1] S. Wadhwa, J. Stöter, F. Zhang, and K. Nayak, “He-HTLC: Revisiting incentives in HTLC,” in *30th Annual Network & Distributed System Security symposium*. NDSS, 2023.

Abstract

Hashed Time-Locked Contracts (HTLCs) are a widely used primitive in blockchain systems such as payment channels, atomic swaps, etc. Unfortunately, HTLC is incentive-incompatible and is vulnerable to bribery attacks. The state-of-the-art solution is MAD-HTLC (Oakland’21), which proposes an elegant idea that leverages miners’ profit-driven nature to defeat bribery attacks.

In this paper, we show that MAD-HTLC is still vulnerable as it only considers a somewhat narrow set of passive strategies by miners. Through a family of novel reverse-bribery attacks, we show concrete active strategies that miners can take to break MAD-HTLC and profit at the loss of MAD-HTLC users. For these attacks, we present their implementation and game-theoretical profitability analysis.

Based on the learnings from our attacks, we propose a new HTLC realization, He-HTLC (Our specification is lightweight and inert to incentive manipulation attacks. Hence, we call it He-HTLC [1] where He stands for Helium.) that is provably secure against all possible strategic manipulation (passive and active). In addition to being secure in a stronger adversary model, He-HTLC achieves other desirable features such as low and user-adjustable collateral, making it more practical to implement and use the proposed schemes. We implemented He-HTLC on Bitcoin and the transaction cost of He-HTLC is comparative to average Bitcoin transaction fees.

DOI Link

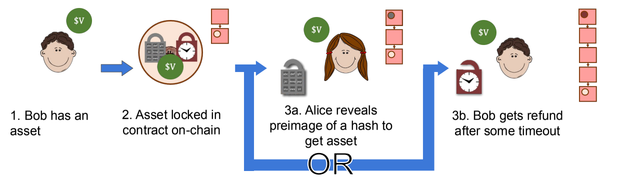
https://dx.doi.org/10.14722/ndss.2023.24775

In Proceedings - NDSS ‘23

He-HTLC: Revisiting Incentives in HTLC

Sarisht Wadhwa (sarisht.wadhwa@duke.edu), Jannis Stöter, Fan Zhang and Kartik Nayak

What is HTLC?



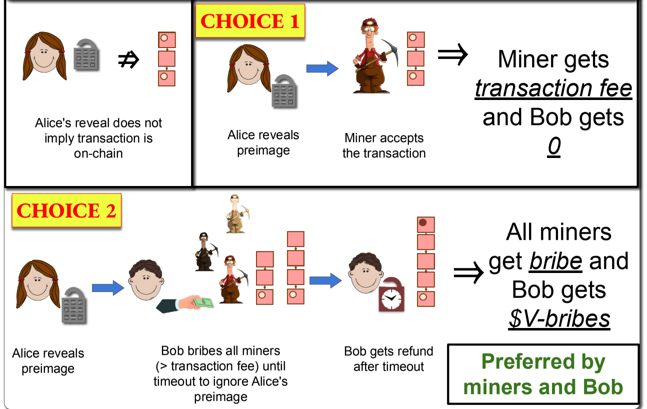
1. Bob has an asset

2. Asset locked in contract on-chain

3a. Alice reveals preimage of a hash to get asset

3b. Bob gets refund after some timeout

Incentive Problems with HTLC



Alice's reveal does not imply transaction is on-chain

CHOICE 1

Alice reveals preimage

Miner accepts the transaction

Miner gets *transaction fee* and Bob gets *0*

CHOICE 2

Alice reveals preimage

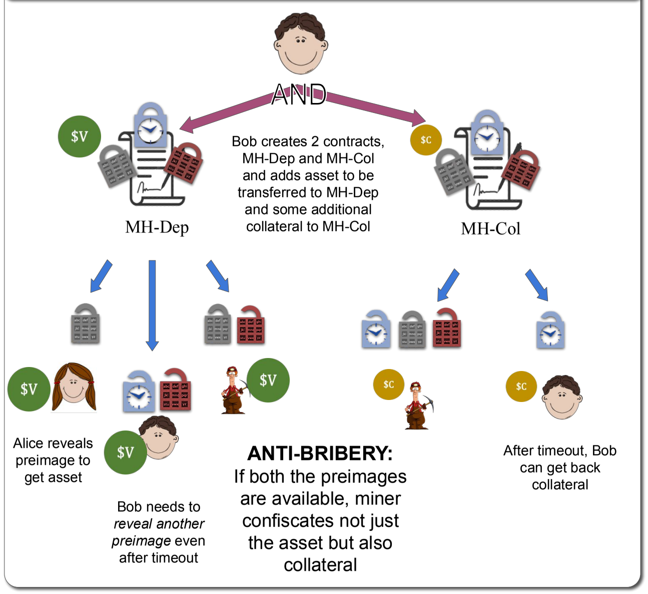
Bob bribes all miners (> transaction fee) until timeout to ignore Alice's preimage

Bob gets refund after timeout

All miners get *bribe* and Bob gets *$V-bribes*

Preferred by miners and Bob

MAD-HTLC [TYME'21]: State of the Art



Bob creates 2 contracts, MH-Dep and MH-Col and adds asset to be transferred to MH-Dep and some additional collateral to MH-Col

Alice reveals preimage to get asset

Bob needs to *reveal another preimage* even after timeout

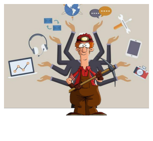
ANTI-BRIBERY: If both the preimages are available, miner confiscates not just the asset but also collateral

After timeout, Bob can get back collateral

Modeling: Active and Passive Miners

Passive miners

- Focused on the mempool
- Confirm most profitable transactions

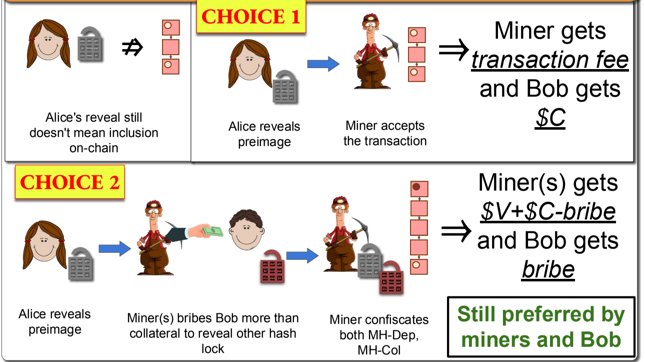


Active miners

- Engage in external protocols
- E.g., add MEV software, open up direct channels to users, etc.

We also need to deal with Active Miners!

Problem in MAD-HTLC: Reverse Bribery



Alice's reveal still doesn't mean inclusion on-chain

CHOICE 1

Alice reveals preimage

Miner accepts the transaction

Miner gets *transaction fee* and Bob gets *$C*

CHOICE 2

Alice reveals preimage

Miner(s) bribes Bob more than collateral to reveal other hash lock

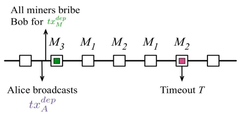
Miner confiscates both MH-Dep, MH-Col

Miner(s) gets *$V+$C-bribe* and Bob gets *bribe*

Still preferred by miners and Bob

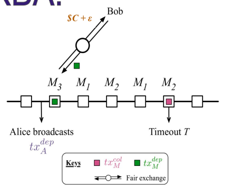
Three Variants of Reverse Bribery

SIRBA:


All miners bribe Bob for tx_M^{dep}
M_3
M_1
M_2
M_1
M_2
Alice broadcasts tx_A^{dep}
Timeout T

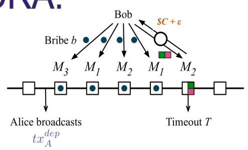
All miners, independent of winning the confiscation transaction, bribe Bob for his secret

SDRBA:



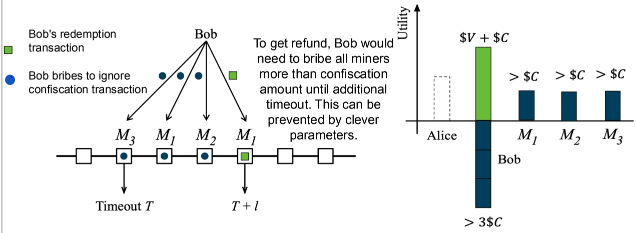
A miner bribes Bob for the secret only when the miner is able to create the block redeeming the deposit. Eliminates risk to miner.

HyDRA:



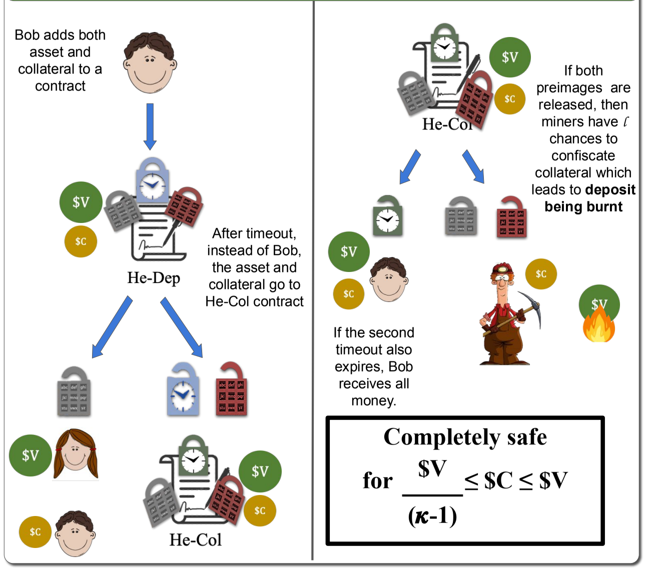
Combining with original bribery attack, to remove dependency on collateral. Modify *SDRBA* to include both collateral and deposit.

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



To get refund, Bob would need to bribe all miners more than confiscation amount until additional timeout. This can be prevented by clever parameters.

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 ℓ chances to confiscate collateral which leads to **deposit being burnt**

If the second timeout also expires, Bob receives all money.

Completely safe for $\frac{\$V}{(\kappa-1)} \le \$C \le \$V$

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.