

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>



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

CHOICE 1

Alice reveals preimage

Miner gets transaction fee and Bob gets Q

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

Miner accepts the transaction

CHOICE 2

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

Bob gets refund after timeout

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

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

After timeout, Bob can get back collateral

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

Bob needs to reveal another preimage even after timeout

Modeling: Active and Passive Miners

Passive miners

used on the pool

firm 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

CHOICE 1

Alice reveals preimage

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

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

Miner accepts the transaction

CHOICE 2

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

Miner confiscates both MH-Dep, MH-Col

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

Still preferred by miners and Bob

Three Variants of Reverse Bribery

SIRBA:

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)

Bob's redemption transaction

Bob bribes to ignore confiscation transaction

Bob's redemption transaction

Miners have 1 chance to ignore confiscation transaction

Miners have 1 chance to ignore confiscation transaction

He-HTLC: An Incentive Compatible HTLC

Bob adds both asset and collateral to a contract

He-Dep

He-Col contract

After timeout, instead of Bob, the asset and collateral go to He-Col contract

If both preimages are released, then miners have 1 chance to confiscate collateral which adds to deposit being burnt

Completely safe for $\$V$ $\$C$ $\$V$ (-1)

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.