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

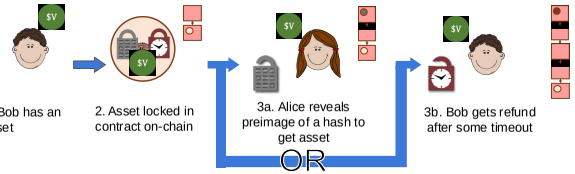
He-HTLC: Revisiting Incentives in HTLC

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

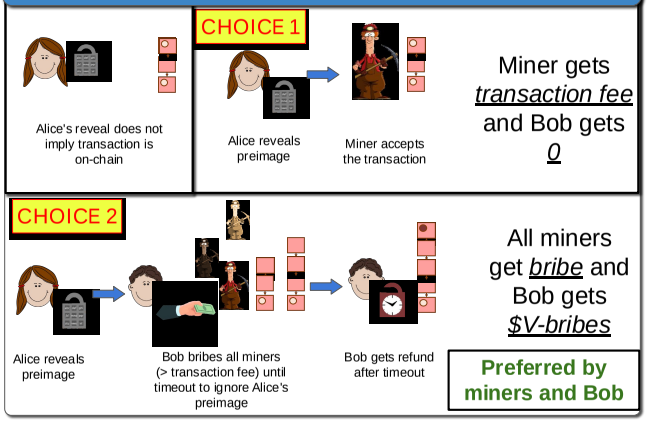
Duke UNIVERSITY

In Proceedings - NDSS '23

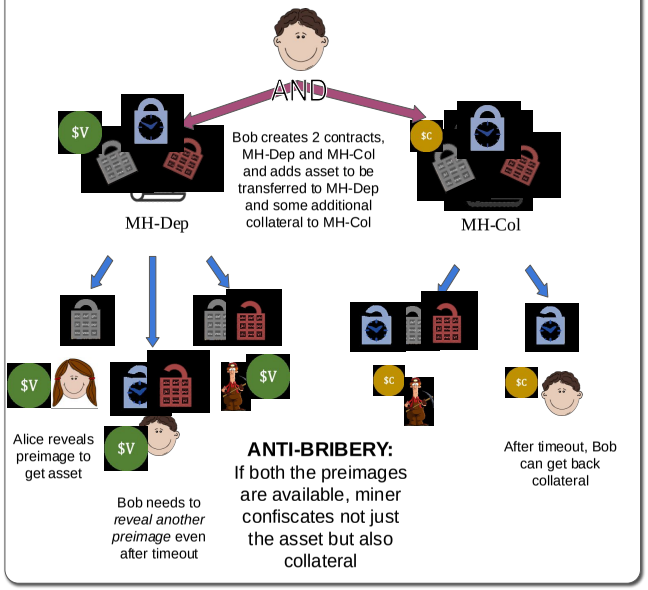
What is HTLC?



Incentive Problems with HTLC



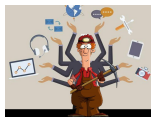
MAD-HTLC [TYME'21]: State of the Art



Modeling: Active and Passive Miners

Passive miners

- …used on the …mpool …nfirm most …fitable …sactions

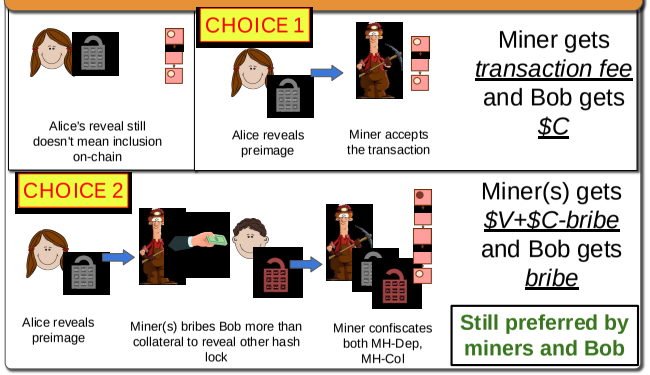


Active miners

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

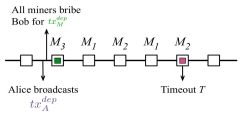
We also need to deal with Active Miners!

Problem in MAD-HTLC: Reverse Bribery



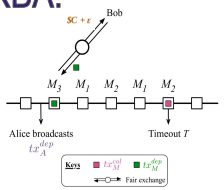
Three Variants of Reverse Bribery

SIRBA:



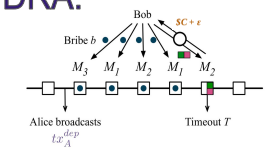
All miners, independent of winning the confiscation transaction, bribe Bob for his secret

SDRBA:



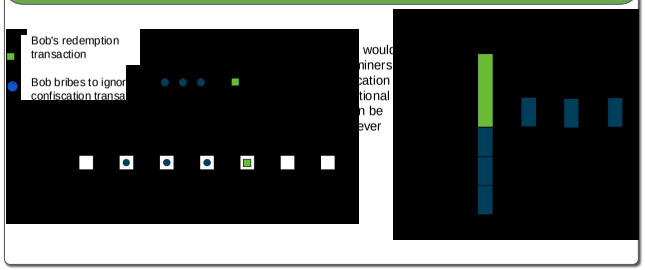
A miner bribes Bob for the secret only when the miner is able to create the block redeeming the deposit. Eliminates risk to miner.

HyDRA:

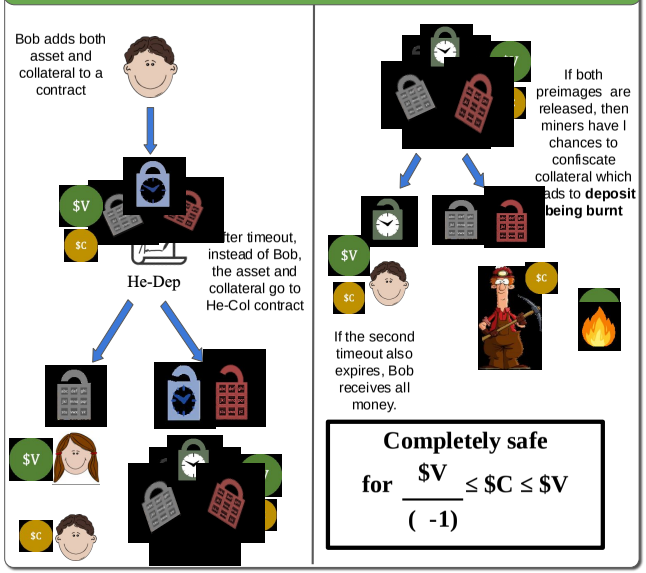


Combining with original bribery attack, to remove dependency on collateral. Modify *SDRBA* to include both collateral and deposit.

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



He-HTLC: An Incentive Compatible HTLC



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.