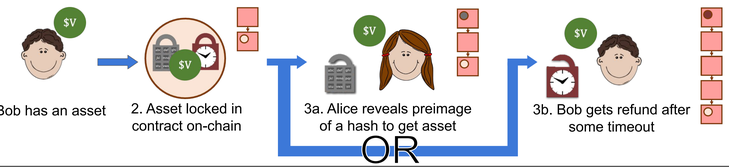
He-HTLC: Revisiting Incentives in HTLC

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

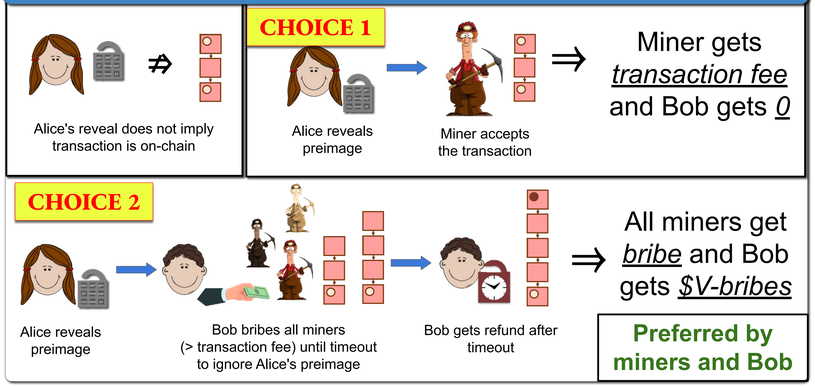
Duke UNIVERSITY

https://eprint.iacr.org/2022/546.pdf

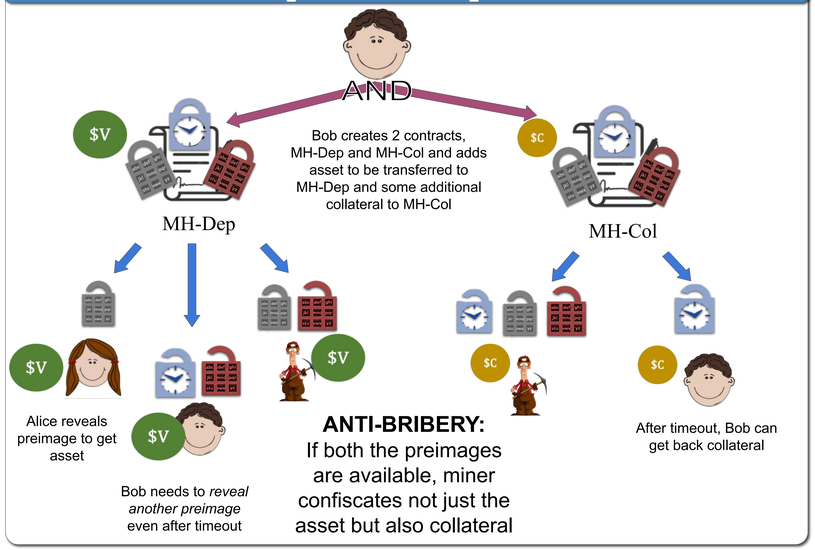
What is HTLC?



Incentive Problems with HTLC



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



Modeling: Active and Passive Miners

Passive miners

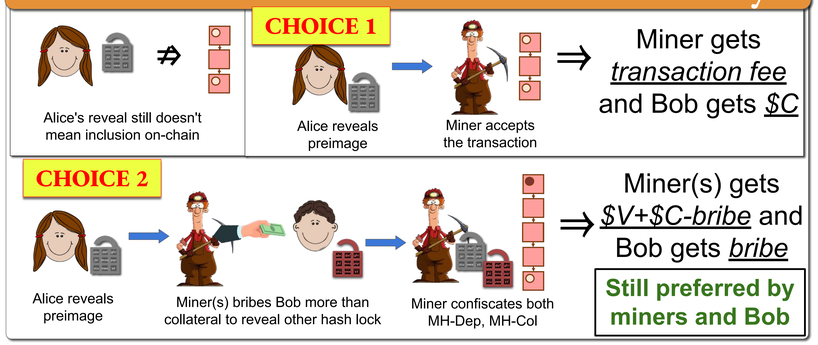
- Focused on the mempool
- Confirm most profitable transactions

Active miners

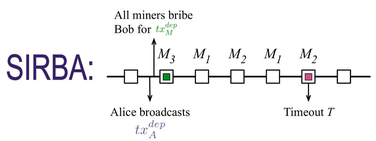
- Engage in external protocols
- E.g., add MEV software, open up direct channels to users, etc.

We also need to deal with Active Miners!

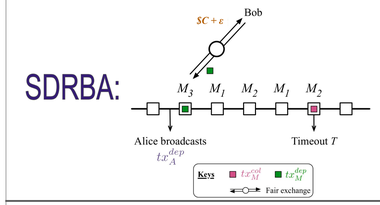
Problem in MAD-HTLC: Reverse Bribery



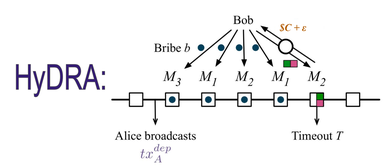
Three Variants of Reverse Bribery



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

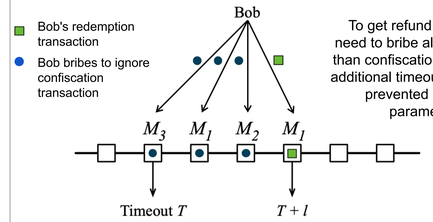


A miner bribes Bob for the secret only when the miner is able to create the block redeeming the deposit. Eliminates risk to miner.

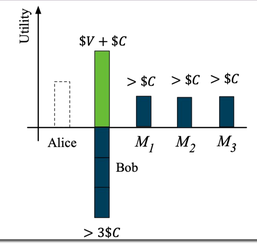


Combining with original bribery attack, to remove dependency on collateral. Modify *SDRBA* to include both collateral and deposit.

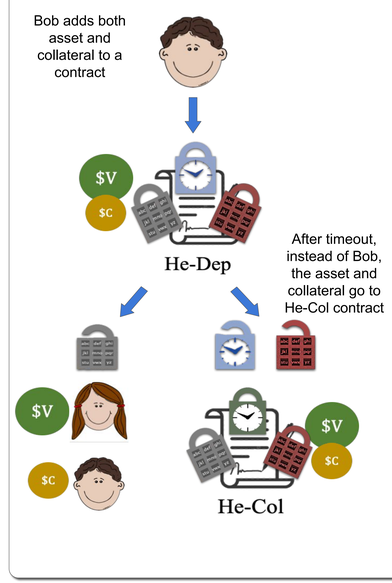
Key Ideas: i) Burn Deposit (Anti-RBA) ii) Use *rationality* of multiple miners (Anti-Bribery)

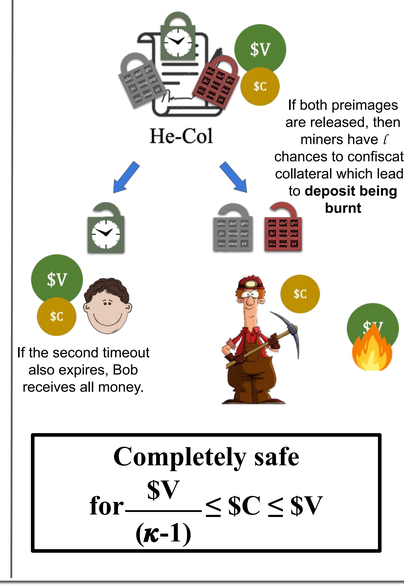


To get refund, Bob would need to bribe all miners more than confiscation amount until additional timeout. This can be prevented by clever parameters.



He-HTLC: An Incentive Compatible HTLC





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

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.