He-HTLC: Revisiting Incentives in HTLC

Sarisht Wadhwa

Joint work with Jannis Stöter, Fan Zhang, Kartik Nayak
Cross-Chain Atomic Swap

**Aim:** Exchange assets on Chain 1 for some assets on Chain 2
HTLC: Hashed Time Lock Contract

Reveal secret to get paid

If no one releases secret until timeout, then refund.
HTLC: Hashed Time Lock Contract

Reveal secret to get paid

If no one releases secret until timeout, then refund.

Bob (Payer) → Deposit/create → Alice (Payee)
HTLC: Hashed Time Lock Contract

Reveal secret to get paid

If no one releases secret until timeout, then refund.
HTLC: Hashed Time Lock Contract

Reveal secret to get paid

If no one releases secret until timeout, then refund.
Cross-Chain Atomic Swap

Both lock their assets in HTLCs using a common hashlock
Cross-Chain Atomic Swap

Both lock their assets in HTLCs using a common hashlock
Cross-Chain Atomic Swap

Both lock their assets in HTLCs using a common hashlock
Cross-Chain Atomic Swap

Bob knows how to open the hashlock, and does so on Bitcoin
Cross-Chain Atomic Swap

Alice learns how to open the hashlock from Bob, and does so for the Ethereum chain.
Cross-Chain Atomic Swap

Alice learns how to open the hashlock from Bob, and does so for the Ethereum chain
Cross-Chain Atomic Swap

If Bob doesn’t reveal the hashlock, then first, timelock on Alice’s contract expires.
Cross-Chain Atomic Swap

If Bob doesn’t reveal the hashlock, then first, timelock on Alice’s contract expires.
Cross-Chain Atomic Swap

Eventually, the other timelock also expires, and Bob gets back the money.
Cross-Chain Atomic Swap

Eventually, the other timelock also expires, and Bob gets back the money
Bribery: A Problem with HTLC [HZ’20, WHF’19]
Bribery: A Problem with HTLC [HZ’20, WHF’19]

Ignore Alice’s TX please :)
Bribery: A Problem with HTLC [HZ’20, WHF’19]

Ignore Alice’s TX please :)
MAD-HTLC [TYME’21]

Make both Alice and Bob loose if anyone cheats – Mutually Assured Destruction

Bob (Payer)  Deposit/create  Alice (Payee)
MAD-HTLC [TYME’21]

Make both Alice and Bob loose if anyone cheats – *Mutually Assured Destruction*
MAD-HTLC [TYME’21]

Make both Alice and Bob loose if anyone cheats – *Mutually Assured Destruction*
MAD-HTLC [TYME’21]

Make both Alice and Bob lose if anyone cheats – Mutually Assured Destruction

Bob (Payer)

| Deposit/create | t > T, Reveal pre(●) |

Alice (Payee)

Both pre(●) and pre(●)

Reveal pre(●)
MAD-HTLC [TYME’21]

Make both Alice and Bob loose if anyone cheats – **Mutually Assured Destruction**

- **Bob** (Payer)
  - $t > T$
  - Reveal $\text{pre}(\bigcirc)$

- **Alice** (Payee)
  - $t > T$
  - Reveal $\text{pre}(\bigcirc)$
  - Both $\text{pre}(\bigcirc)$ and $\text{pre}(\bigcirc)$

- Deposit/create

- Reveal $\text{pre}(\bigcirc)$
**MAD-HTLC** [TYME’21]

Make both Alice and Bob loose if anyone cheats – *Mutually Assured Destruction*

This **defeats** Bob’s bribery because:

- Bob must reveal `pre(●)` to realize profit and then miners will grab everything.

Bob (Payer)

Alice (Payee)
Contributions: Revisiting Incentives in HTLC

Attacks on HTLC Schemes
- Notion of actively rational miners
- Three reverse bribery attacks (RBA)
  - Success Independent RBA
  - Success Dependent RBA
  - Hybrid Attack

He-HTLC
An incentive-compatible HTLC scheme
MAD-HTLC: Is it Safe?

For a miner, achieving the following state is the best-case scenario.

Bob (Payer)

Deposit/create

t > T,

Reveal pre(·)

Alice (Payee)

Reveal pre(·)

Both pre(·) and pre(·)

For a miner, achieving the following state is the best-case scenario.

Both pre(·) and pre(·)

Both pre(·) and pre(·)
MAD-HTLC: Is it Safe?

For a miner, achieving the following state is the best-case scenario.

Are there some actions miner can take to ensure this state?
Passive vs Active Miners

**Passive miners**
- Focused on the mempool
- Confirming most profitable transactions

**Active miners**
- Engage in external protocols
- E.g., adding MEV software, open up direct channels to users, etc.
Reverse Bribery: Active Miners’ Action

Bob (Payer)

Deposit/create

Reveal $\text{pre}(\text{ })$

Alice (Payee)
Reverse Bribery: Active Miners’ Action

Bob (Payer)

Deposit/create

$t > T,$

Reveal $\text{pre}(\ )$

Reveal $\text{pre}(\ )$

Alice (Payee)

$\$R_B$
Reverse Bribery: Active Miners’ Action

Bob (Payer)

Deposit/create

Reveal pre

Both pre and pre

$R_B > C$

Alice (Payee)
Attacks Based on Reverse Bribery (RBA)

- Success Independent RBA
Attacks Based on Reverse Bribery (RBA)

- Success Independent RBA
- Success Dependent RBA
Attacks Based on Reverse Bribery (RBA)

- Success Independent RBA
- Success Dependent RBA
- Hybrid Delay-Reverse Bribery Attack
Attacks Based on Reverse Bribery (RBA)

- Success Independent RBA
- Success Dependent RBA
- Hybrid Delay-Reverse Bribery Attack

For details, let’s chat in the poster session. (Poster 46)
Designing HTLC: Challenges

**Bribery Resistance**: The payer must have a way to get back all the money ($V + $C) after the timeout.
Designing HTLC: Challenges

Bribery Resistance: The payer must have a way to get back all the money ($V + $C) after the timeout.

😊 Payer must not be able to bribe a miner more than what the miner receives as enforcer.
Designing HTLC: Challenges

- **Bribery Resistance:** The payer must have a way to get back all the money ($V + $C) after the timeout.

  😞 Payer must not be able to bribe a miner more than what the miner receives as enforcer.

- **Reverse Bribery Resistance:** In MAD-HTLC miner earns too much when punishing bribery attempts.
Designing HTLC: Challenges

**Bribery Resistance:** The payer must have a way to get back all the money ($V + $C) after the timeout.

😊 Payer must not be able to bribe a miner more than what the miner receives as enforcer.

**Reverse Bribery Resistance:** In MAD-HTLC miner earns too much when punishing bribery attempts.

😢 A miner must receive $\leq C$. 
Designing HTLC: Key Ideas

- **Bribery Resistance:** The payer must have a way to get back all the money ($V + C) after the timeout.

  Make payer bribe multiple miners, so that not all of them can be bribed!

- **Reverse Bribery Resistance:** In MAD-HTLC miner earns too much when punishing bribery attempts.

  🙁 A miner must receive $\leq C$. 
Designing HTLC: Key Ideas

**Bribery Resistance:** The payer must have a way to get back all the money ($V + C$) after the timeout. Make payer bribe multiple miners, so that not all of them can be bribed!

**Reverse Bribery Resistance:** In MAD-HTLC miner earns too much when punishing bribery attempts. Burn the deposit ($V$) to avoid reverse bribery.
He-HTLC: An Incentive Compatible HTLC

✓ No incentive-based attacks on HTLCs even with 100% active miners!
He-HTLC: An Incentive Compatible HTLC

✓ No incentive-based attacks on HTLCs even with 100% active miners!

✓ Low and user adjustable collateral ($C < \$V$)
He-HTLC: An Incentive Compatible HTLC

✓ No incentive-based attacks on HTLCs even with 100% active miners!

✓ Low and user adjustable collateral ($C < V$)

✓ A lightweight Bitcoin implementation (no new op-codes)
Thank You!

Contact: sarisht.wadhwa@duke.edu
He-HTLC: Revisiting Incentives in HTLC

Sarisht Wadhwa
Duke University
sarisht.wadhwa@duke.edu

Jannis Stöter
Duke University
jannis.stoeter@alumni.duke.edu

Fan Zhang
Duke University
fan.zhang@duke.edu

Kartik Nayak
Duke University
kartik@cs.duke.edu

Thank You!

In proceedings for NDSS’23...

Contact: sarisht.wadhwa@duke.edu