cryptoeconomics.study

An intro course on mechanism design for blockchains

Incentive Case Study

HTLCs and the Free Option Problem

What’s an HTLC?

HTLC stands for “Hashed Timelock Contract”

It’s a type of contract that uses:

Hashlocks to restrict the spending of a contract until the preimage of the hash is revealed.

Timelocks to restrict the transfer of cryptocurrency until a specified time or blockheight, and as a failsafe in an emergency.

What do HTLCs enable?

- Enables users to opt-in to payments
- Enables payment routing through multiple hops
- Enables conditional payments
- Enables a new class of conditional payments

Bitsy and Ethel’s Currency Swap

Ethel Ethereum and Bitsy Bitcoin want to use an HTLC to exchange bitcoin for ethereum.

Ethel Ethereum

Bitsy Bitcoin

Before the swap, off chain agreements that must be made:

- Agree to an exchange rate
- Agree to a timeout
- Agree on a hash

Ethel

Bitsy

Bitsy and Ethel’s Currency Swap

Ethel takes lead in generating a preimage, which she hashes and gives the hash to Bitsy.

Bitsy and Ethel's Currency Swap

Ethel and Bitsy each deploy and lock funds into their respective contracts with the agreed-upon parameters:

fx rate, hash, timelock

Bitsy and Ethel’s Currency Swap

Now, in order to claim the bitcoin, Ethel must send the preimage to btc_contract that Bitsy deposited bitcoin in.

If Ethel sends the preimage to btc_contract, Bitsy can copy it and send it to eth_contract that Ethel deposited ETH in, so Bitsy can claim her ETH.

Ethel’s Betrayal

Claims

Claim 1: “Griefing in this manner would affect your reputation, so the exchange or the other party can just choose not to transact with you.”

Claim 2: “Time-outs are short so it’s not really a free option and therefore not a problem.”

Concerns with Claim 1

Claim 1: “Griefing in this manner would affect your reputation, so the exchange or the other party can just choose not to transact with you.”

Concern:

- **As anonymity increases, this becomes more tenuous (atomic swaps on a DEX)**
- **The lower the cost of creating identities, the more tenuous this becomes**

Concerns with Claim 2

Claim 2: “Time-outs are short so it’s not really a free option and therefore not a problem.”

Concern:

- **Independent time systems process time relatively and asynchronously, so long timeouts are required to make sure there is enough time overlapping that players have time to publish on both chains in worst case scenarios (adversarial conditions)**

Potential Solution Paths

- Streaming micropayments as proposed by interledger
- Only transact with whitelisted addresses
- Cryptoeconomics.study

Thanks to Jeremy Rubin, Evan Schwartz, Karl Floersch and Dan Robinson for the analyses on HTLCs

cryptoeconomics.study

An intro course on mechanism design for blockchains