Fair Atomic Swaps

Lloyd Fournier

Introduction

Atomic swap protocols allow participants to exchange ownership of assets across blockchains without a trusted third-party. They are often touted as a way to replace centralized exchanges altogether. Unfortunately, the most widespread protocol among the cryptocurrency community is *unfair*[1, 2] - one party may abort to their own financial advantage. We propose a novel *fair atomic swap* protocol that addresses this flaw by identifying and punishing unfair behaviour. We then show how to modify the construction to create a cross-chain option contract.

Unfair Atomic Swaps

Consider two parties who wish to exchange ownership of assets across blockchains. Alice owns an asset $\mathbf{A}$ on ledger α and Bob owns an asset $\mathbf{B}$ on ledger β. To make the exchange *atomic*, Alice's transfer of $\mathbf{A}$ to Bob must be conditioned on Bob's transfer of $\mathbf{B}$ to Alice. The most widespread protocol (Figure 1) uses Hash Time Locked Contracts (HTLC) to communicate the outcome of the protocol from β to α to enforce this condition [3]. A HTLC locks an asset until either the *redeemer* unlocks the asset by providing the secret pre-image to the hash or the *refunder* retrieves the asset after an expiration time.

Figure 1:Atomic Swap Protocol - by Tier Nolan [3]

The issue with this protocol is that if Alice perceives that $\mathbf{B}$ has declined in value relative to $\mathbf{A}$ once the β HTLC has been confirmed she can decide not to redeem it and instead wait to refund ownership of the more valuable $\mathbf{A}$. We cannot reduce the β expiry to limit her ability to do this without harming the security of the protocol for an honest Alice. This problem is often called the *Free Option Problem* [1], because Alice gets what amounts to an American-style option without paying a premium.

Fair Atomic Swaps

In addressing the fairness issue, our first key observation is that whenever someone makes an *offer* to do some asset exchange, they must be able to cancel it. Not being able to cancel an offer is essentially the definition of giving someone a free option. We need a protocol structure that follows intuitively from how trades on exchanges actually work:

Two-party Asset Exchange

`MakeOffer`: Alice can make an offer to Bob to trade some asset $\mathbf{A}$ for some asset $\mathbf{B}$.
`TakeOffer`: Bob can take the offer (unless Alice has canceled it). This executes the change in ownership.
`CancelOffer`: Alice can cancel her offer (unless Bob has taken it).

Our second observation is that we can punish the unfair behaviour. There is a well developed line of research (starting in [4] and most recently [5]) that uses a blockchain to counter unfair behaviour in multi-party computation. The basic idea is to identify and punish bad behaviour so that it will be in the interest of all participants to execute the protocol honestly. To apply this idea we require that Alice must own some asset $\mathbf{C}$ on β such that its loss will overwhelm any benefit she could gain by aborting the protocol.
The fair atomic swap is illustrated in Figure 2. Only the β ledger part is displayed because the α ledger protocol is unchanged.

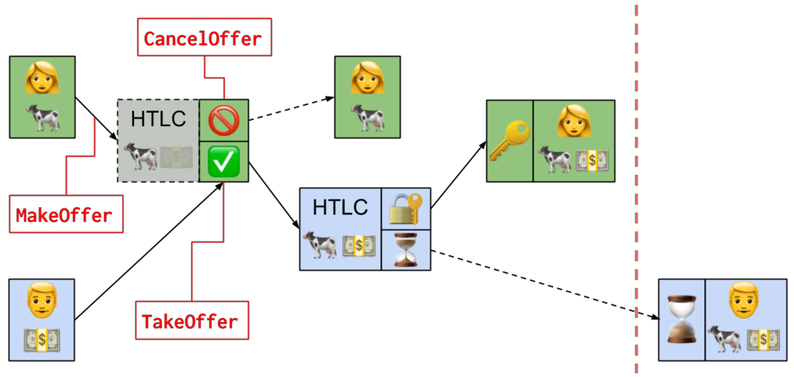

Figure 2:The β ledger part of the fair atomic swap protocol

[1] ZmnSCPxj, "An argument for single-asset lightning network." `https://tinyurl.com/ydda5z9t`.
[2] D. Robinson, "HTLCs Considered Harmful." `https://tinyurl.com/yctcwjqv`.
[3] T. Nolan, "Alt chains and atomic transfers." `https://tinyurl.com/ycundcpe`.
[4] M. Andrychowicz, S. Dziembowski, D. Malinowski, and L. Mazurek, "Secure multi-party computations on bitcoin," 2013. `https://tinyurl.com/y9fkhnwd`.
[5] C. Baum, B. David, and R. Dowsley, "Insured mpc: Efficient secure multiparty computation with punishable abort," 2018. `https://tinyurl.com/y9nj4l8d`.

Example in Bitcoin

If we instantiate β with the Bitcoin Blockchain and set Bob's asset $\mathbf{B} = 10$ BTC and Alice's collateral $\mathbf{C} = 1$ BTC the Two-party Asset Exchange can be described as:

- `MakeOffer` Alice signs a transaction with the `SIGHASH_SINGLE` signature flag. This allows her to sign only one input and one output. The input is 1 BTC from an output she owns and the output is the 11 BTC HTLC (where she is the redeemer). She then sends this incomplete transaction to Bob.
- `TakeOffer` If Bob wants to take Alice's offer, he takes the transaction and finishes it by adding another input of 10 BTC (plus some fee) and sends it to the Bitcoin Blockchain.
- `CancelOffer` If Alice wishes to cancel her offer to Bob she tries to double spend the 1 BTC output so that Bob will be unable to `TakeOffer`.

Fair Cross-chain Options

It is simple to transform the fair atomic swap protocol into a cross-chain option protocol (Figure 3). The construction takes the same shape except as soon as Bob does `TakeOffer` he receives $\mathbf{C}$ immediately regardless of Alice's decision to exercise her option or not. This transforms $\mathbf{C}$ from collateral into an option premium.

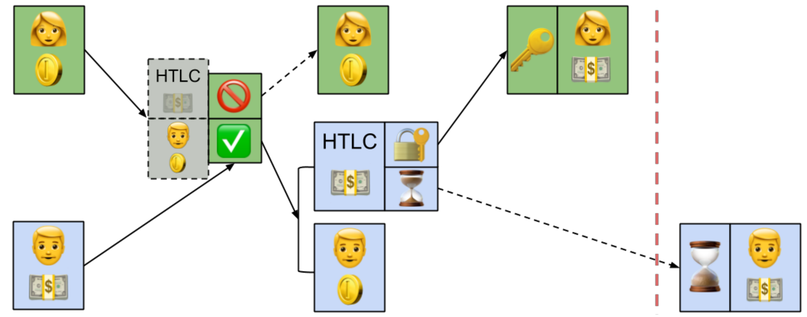

Figure 3:The β ledger part of the Fair Option protocol.

Contact Information

Lloyd Fournier lloyd@coblox.tech
Philipp Hoenisch philipp@coblox.tech
CoBloX https://coblox.tech
Blog https://blog.coblox.tech
COMIT https://comit.network