Atomic Swaptions: Cryptocurrency Derivatives

James A. Liu
Department of Computer Science
University of California, Irvine
jamesal1@uci.edu

July 24, 2018

Abstract

The atomic swap protocol allows for the exchange of cryptocurrencies on different blockchains without the need to trust a third-party. However, market participants who desire to hold derivative assets such as options or futures would also benefit from trustless exchange. In this paper I propose the atomic swaption, which extends the atomic swap to allow for such exchanges. Crucially, atomic swaptions do not require the use of oracles. I also introduce the margin contract, which provides the ability to create leveraged and short positions. Lastly, I discuss how atomic swaptions may be routed on the Lightning Network.

1 Trustless Exchange

Cryptocurrencies such as Bitcoin rely on cryptographic protocols for security. However, as originally designed, there was no mechanism for different blockchains to communicate securely with each other. Thus, cryptocurrency trading is done "off-chain", or outside of the scope of the blockchains involved. Two users who wish to trade have to deposit their funds into a trusted third party, typically taking the form of a centralized cryptocurrency exchange.

The need to trust centralized exchanges has long been an uncomfortable reality within the cryptocurrency community. Exchange participants often fear that their funds may be frozen, seized or stolen, and history has shown that such fears are well-founded[1]. Conversely, exchanges with good reputations have monopolistic power over potential new users/investors of a given cryptocurrency, allowing them to extract rents and exercise undue influence over cryptocurrency development in general. For instance, they can choose which new altcoins to support on their exchange, perhaps charging a listing fee. Creators of new altcoins must cede to their demands or take their chances by working with less reputable exchanges. These frictions make it difficult for new participants to acquire coins, posing an impediment to the adoption of cryptocurrencies.

The volatility of cryptocurrencies provides another impediment to their adoption, gamblers and speculators notwithstanding. Potential users might be more inclined to adopt a given cryptocurrency if they were able to hedge its volatility risk through the use of financial options or futures markets. For example, producers of cryptocurrencies (i.e. miners) have revenues denominated in cryptocurrency, but generally have expenses denominated in various fiat currencies. However, relying on centralized exchanges for derivatives trades would expose users to the same problems that spot traders face. In fact, these problems would be magnified. The long-term nature of derivatives means that users would have to keep their assets on the exchange for the entire length of the contract. In addition, any leverage offered by the exchange would lead to direct and indirect counterparty risk; the exchange may enter into one-sided bets or be lax in enforcing margin for some of its users. In the case of extreme market fluctuations, the exchange may become insolvent.

The atomic swap allows users to avoid the risks and disadvantages inherent to centralized exchanges when trading. Atomic swaps use Hashed Time Lock Contracts (HTLCs), a form of cryptographic escrow; the blockchains themselves act as the trusted third party. Viewed another way, atomic swaps utilize cryptographic secrets to allow users to prove on one blockchain that certain events occurred on a different blockchain.

In this paper I demonstrate that the functionality of atomic swaps can be further extended to allow the creation of option contracts, which I term atomic swaptions. In particular, parties can deposit only a fractional margin instead of the full principal. This, in turn, allows for a meaningful notion of a futures contract, enabling users to take leveraged or short positions on one cryptocurrency against another.

1.1 Related Work

Related approaches to decentralized cryptocurrency derivatives focus on trading ERC20 tokens on the Ethereum blockchain [2] [3] and/or use oracles (trusted providers of external data) to determine contract outcomes [4]. In contrast, the approach I outline can be used between different blockchains, with only the requirement that they can support the creation of HTLCs with the same hash function. Namely, the blockchains don't need to be Turing-complete like Ethereum. In addition, atomic swaptions don't require oracles, eliminating an unnecessary element of trust from the process.

Others have also modified atomic swaps to create basic option contracts [5] [6]. However, the construction they use has a serious drawback: if either party reneges, the participants can't get refunded until option expiration. Also, my approach is more flexible, allowing for the various modifications described in this paper.

2 Layout

In this paper, I review how atomic swaps work, then show how atomic swaptions naturally arise as an extension of them. I show how various features can be implemented, such as early cancellation and margin. Furthermore, I discuss how atomic swaptions could be used in practice. In particular, I discuss how they may be implemented on the Lightning Network, as well as the general ramifications of having long-term contracts on the Lightning Network. Finally, I note some of the risks and limitations of atomic swaptions.

In the example transactions I use, Alice initially possesses ACoin and Bob initially possesses BCoin, placeholder cryptocurrencies that live on different blockchains with functionality equivalent to Bitcoin. Alice plays the role of swaption buyer, while Bob plays the role of swaption seller.

Contract diagrams are in the appendix; readers are encouraged to refer to the appendix to aid their understanding of the overall structure.

3 Atomic Swap

Suppose Alice wants to trade her ACoin for Bob's BCoin. If she were to send her Acoin to Bob first, Bob could then simply drop out of the process without sending any BCoin to her, and vice versa if Bob sends his BCoin first. Instead, Alice and Bob can use an atomic swap, which doesn't require either party to trust the other to act honestly. First, they construct a Hashed Time Lock Contract (HTLC) for Alice's ACoin. Omitting the implementation details, the HTLC allows Bob to take the ACoin if he can provide the secret value A, which only Alice knows. It also allows Alice to take back the ACoin after expiration time $T+1$, in case Bob drops out. Once the ACoin has been sent to the HTLC, Bob deposits his BCoin into a similar HTLC set to expire at time T, so that it expires before Alice's does. This allows him to reclaim the BCoin if Alice fails to reveal A. If she publishes the transaction to take the BCoin, then in doing so she reveals A; Bob can then use A to take the ACoin, completing the swap.

4 Atomic Swaption

Notice that Alice is able to purposefully renege on the trade after Bob deposits his BCoin. She may do this if the price of ACoin has gone up relative to BCoin after she and Bob have agreed to trade. In fact, she has until the expiration of the contract to decide whether or not to go through with the trade. Bob is locked into the trade; he receives the coins that Alice considers less valuable.

In other words, the atomic swap can be seen as a financial option allowing Alice the ability to trade ACoin for BCoin at a fixed price, which has value for Alice. For small values of T, this "option value" will generally be small, as it is unlikely that market prices will change greatly in a short period of time.

If T were large, then Alice would gain significant option value. In return, Alice could pay Bob a premium to enter into this so-called swaption contract (an option to do a swap). The question arises as to how the swaption can be exchanged securely for the premium. This is done by nesting the swaption into another atomic swap. In this example, Alice pays the premium in ACoin, but she could also pay using an arbitrary cryptocurrency, since atomic swaps can involve an arbitrary number of blockchains.

This framework allows for some variations. For example, a compound option is simply an option on an option, so it can be implemented through further nesting of HTLCs. Similarly, a collar option strategy can be implemented efficiently through nesting rather than by trading multiple swaptions. It is even possible to create an option to enter into a discreet log contract. Here, I analyze early cancellation and margin, as they are likely to be very useful for swaption traders.

4.1 Early Cancellation

Suppose Alice would like to be able to forfeit the swaption and reclaim her ACoin early. It's possible to design the refund transactions to allow Alice and Bob to cancel the swaption, but Bob may be uncooperative and force Alice to wait until expiration. Instead, the swaption can be configured so that Alice can use another secret to cancel it. To ensure that Alice does not try to simultaneously exercise and cancel the swaption, the funds are sent to Revocable Sequence Maturity Contracts. The RSMC corresponding to Alice's exercise transaction allows Bob to take the BCoin if Alice also published the cancel transaction, and vice versa. Thus, if Alice tries to cheat, Bob can take all of the funds as punishment.

4.2 Margin

Instead of depositing all of their funds into the contract, Alice and Bob can agree to deposit only a fraction (”margin”) of the total funds (”principal”). This is achieved through the use of a margin contract. Bob's margin contract allows him to send the margin to the swaption contract, but the transaction that allows him to do this specifies that the output is equal to the full principal, thus requiring that he also deposit the rest of the funds as well. In Bitcoin, this is best achieved through use of SIGHASH_ANYONECANPAY. Blockchains with different scripting rules may require Bob to send the principal remainder to a placeholder contract first.

If Bob does not deposit funds into the swaption contract by the margin expiration, Alice can take the margin funds, and does not need to reveal any secret to do so, meaning that she can also take back her ACoin by not exercising. Alice's margin contract functions similarly, but should expire before Bob's margin contract does. If she fails to deposit the principal, then Bob can take her margin, and forfeit his own.

It should be noted that Alice's margin deposit is only necessary due to the limitations of HTLCs as a communication protocol between blockchains. That is, Bob cannot prove on the BCoin blockchain that Alice *didn't* deposit funds into the ACoin swaption contract (and Alice cannot prove on the BCoin blockchain that she *did* deposit the ACoin). If this were possible, then Alice's exercise transaction, which occurs on the BCoin blockchain, could be prevented until she deposited her ACoin into the ACoin swaption contract. If, however, ACoin and BCoin were on the same blockchain (e.g. they were both ERC20 tokens), then the contract could be designed so that Alice would not need to deposit any funds until she decides to exercise.

When negotiating terms, Alice and Bob should take into account the possibility of strategic default, which changes the payoff function of the swaption. Setting Alice's margin-to-principal ratio to be equal to Bob's is sufficient to ensure that Alice never has an incentive to default; however, unless Bob's margin is equal to the principal, there are situations in which he is incentivized to default. In light of this, I outline two possible approaches to designing swaptions on margin, with equal margin ratios between Alice and Bob. The fixed margin approach is essentially "set and forget"; once the swaption is set up, Alice and Bob don't need to take any action until the swaption is about to expire. The floating margin approach tries to closely replicate the traditional payoff function of a call or put option, but requires frequent interaction between Alice and Bob.

4.2.1 Fixed margin swaption

Here, the margin expiration M is set right before the swaption expiration ($E - 2$ at the latest), so that Bob decides at expiration whether or not to default. Let m_B, p_B correspond to the amount of BCoin margin and principal, and likewise for p_A. The intrinsic value of the swaption is then given by $max(0, min(m_B, p_B - p_A))$, not including the value of the margin deposit. This leads to the kinked payoff function shown in Figure 1; it can be decomposed into two traditional options for the purposes of pricing.

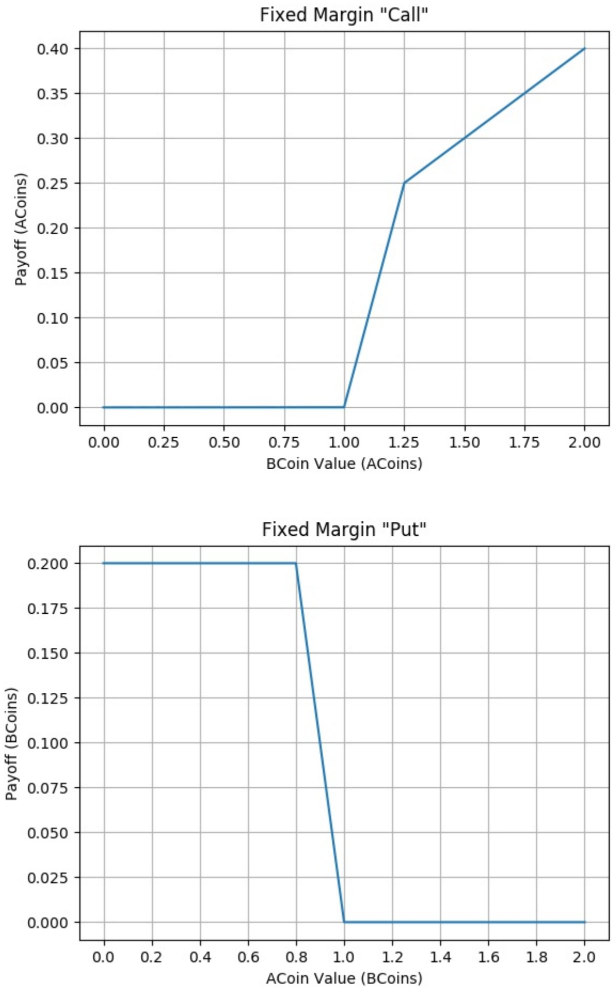


Figure 1: Fixed margin swaption payoff functions. Note that both graphs describe the same swaption. When denominated in ACoin it is a call option; when denominated in BCoin, it is a put option.

4.2.2 Floating margin swaption

Here, Alice and Bob can agree to continuously ”mark to market” the option, increasing or decreasing the amount of margin required such that the expected gain from strategic default is below a small, pre-determined threshold. This is done by atomically cancelling the old swaption while creating the new swaption. The margin expiration is set to an intermediate value M, perhaps ranging from a day to a week. If Alice and Bob cooperate, the time until the margin expiration will continuously be reset to this value, but if one party stops cooperating (such as in a dispute about the marking), then the two parties have time to come up with the funds to avoid defaulting. The choice of M is a tradeoff; a smaller value of M allows for smaller margin and/or a lower probability of strategic default, but provides less time to respond in the non-cooperative case.

Floating margin is best done on a "layer 2" off-chain scaling solution such as the Lightning Network, which allows users to make secure contracts without having to publish any transactions, except in the case of cheating. Otherwise, it could be very expensive to repeatedly create and cancel swaption contracts using on-chain transactions.

4.2.3 Futures

Since floating margin faithfully replicates the payoff of a call/put option, it can be used for the creation of futures contracts. A version of put-call parity states that a long futures contract is equivalent to a long call option and short put option position (disregarding early exercise). In other words, to create a futures contract, Alice and Bob can atomically open two floating margin swaptions simultaneously with the same strike price and expiration, allowing Alice to swap 1 ACoin for 1 BCoin and allowing Bob to swap 1 BCoin for 1 ACoin. Note that this construction is non-trivial because Alice contributes ACoin to both contracts. The strike price should be kept close to the futures market price (more correctly, the expected spot price at expiration), in order to minimize the amount of margin needed.

5 Lightning Network Routing

Note that much of this analysis can be applied to other long-term contracts such as discreet log contracts, which are easier to handle since they only pertain to one blockchain.

It is possible for Alice and Bob to enter into swaption contracts through intermediate participants on the Lightning Network, in the same way that they could perform an atomic swap by chaining Hashed Time Lock Contract (HTLC) ACoin payments going from Alice to Bob and looping back with BCoin payments.

As each step of the swaption consists of a HTLC and/or a contract sending to a HTLC, it is straightforward to implement atomic swaptions on LN, by adding Revocable Sequence Maturity Contracts as needed. Deviating actions by intermediaries are unprofitable and will not result in loss for other participants. It should also be clear that several HTLCs can be open simultaneously on a payment channel. Therefore, long-running swaptions don't disrupt operation of the channels, beyond the specific amount of funds that have to be tied up in the swaption contract.

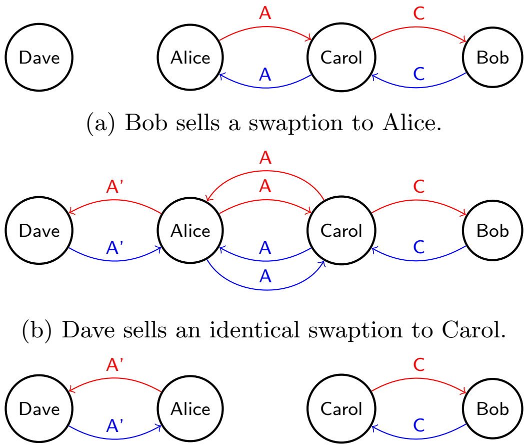
Within a payment channel, users only need enough funds to cover the margin to participate in a swaption contract. However, they may have to close the payment channel in order to pay the principal if they don't have enough funds in the channel.

5.1 Third Party Decoupling and Unwinding

If a third party, Carol, has nodes appearing on both the ACoin and BCoin paths between Alice and Bob, she can instead decouple the swaption, using her own secret with Bob. In this case, Carol functions as counterparty to both Alice and Bob (or to other intermediaries acting similarly), and has zero net position. This lowers the required time for swaption exercise (since each step of a chain of HTLC payments must expire 1 timestep later). Furthermore, Carol can unilaterally close her long option position with Bob without waiting for Alice to do so, freeing up her funds sooner. In the fully cooperative case, it also simplifies the option unwinding process.

Suppose now that an identical trade passes through Alice and Carol such that Carol would open a long position against Alice. Since Alice and Carol would now have a net zero position against each other, it would be ideal to end the process such that both swaptions have been cancelled, so that their funds are not locked up needlessly. Carol can set her swaption with Alice to expire 1 timestep after Alice's swaption with her, using the same secrets. Alice would then reveal her secret, causing a circular flow of funds that can be undone with cyclic rebalancing.

Similarly, by using self-trading, existing positions can be rerouted, such as when two parties want to close their channel without putting any contracts onto the blockchain. Use of these techniques can help minimize the costs of keeping the chain of swaption positions open on the LN.



(a) Bob sells a swaption to Alice.

(b) Dave sells an identical swaption to Carol.

(c) Alice and Carol cancel their swaptions.

5.2 Economic Considerations

Long paths are likely to be expensive, as Alice and Bob will have to compensate all of the intermediaries for the time value of their locked-up funds, as well as for taking on the risks and possible network transaction fees inherent in the process. Note also that intermediaries will have to maintain sufficient liquidity in order to avoid defaulting on margin swaptions, and need to be compensated for this. Swaptions, DLCs, and other long-term contracts all compete for the same network fund capacity.

This suggests that LN-based derivatives trading will mostly be fairly centralized, with a small set of densely connected large traders/exchanges, and many smaller traders directly connected to the large traders.

The ability to unwind identical swaptions encourages standardization of contract terms such as strike price, size, expiry, etc.

6 Practical Considerations

As with other long-term contracts, there is a risk that there is an emergency rule change on one of the blockchains, such as in the hashing or signing algorithm. Presumably, unmoved coins will be burned (rendered unspendable). There are a few possibilities for Alice and Bob; the dynamics are influenced by the particular contract and the timing of the rule change. They may cooperate and reopen the contract under the new rules, possibly with one party extorting the other for an excess payment. If Bob isn't cooperative, Alice must choose between exercise or cancelling by the move deadline, forfeiting the extrinsic value of the swaption. However, Alice can also harm Bob by not acting until the compromised coins are burned, then taking the coins from the other blockchain.

Leveraged trading is unlikely to be user-friendly, as it may require a good deal of familiarity with options pricing formulas/software. In addition, users of margin should not rely on their counterparty being cooperative, as the counterparty often stands to gain substantially if margin is forfeited. It is even possible that, given a substantial enough swaption market, manipulators will attempt to orchestrate "short squeezes" by accumulating large swaption positions whose margin expirations occur at the same time. They may be aided through use of long paths of intermediaries on LN.

Timelocks must be set to use time elapsed rather than block height, so that the timelocks expire in the intended order; it is difficult to predict the relative timing of future blocks between two different blockchains. Of course, it's not clear that many users would prefer to use block height if it were possible.

There have been a variety of attempts to create cryptocurrencies pegged to fiat currencies. Users seeking to minimize volatility will likely prefer to use pegged cryptocurrencies in their swaption trades, though this of course requires them to trust in the underlying peg.

7 Conclusion

The design and adoption of new blockchains is an ongoing process, and it remains an open question what operations a blockchain should support to best facilitate the development of applications on top of it. I have demonstrated that a wide class of inter-blockchain derivatives can be implemented with only the features required to implement an atomic swap. The atomic swaption thus provides a practical path to derivatives trading on existing cryptocurrencies, and removes the need for designers of future blockchains to create specialized derivatives applications.

References

[1] Andrea Tan and Yuji Nakamura. Cryptocurrency markets are juicy targets for hackers: Timeline. `https://www.bloomberg.com/news/articles/2018-01-29/cryptocurrency-markets-are-juicy-targets-for-hackers-timeline`. Accessed: 2018-07-10.

[2] Antonio Juliano. dydx: A standard for decentralized derivatives. April 24, 2018.

[3] Shayan Eskandari, Jeremy Clark, Vignesh Sundaresan, and Moe Adham. On the feasibility of decentralized derivatives markets. *CoRR*, abs/1802.04915, 2018.

[4] Thaddeus Dryja. *Discreet Log Contracts.* MIT Digital Currency Initiative.

[5] Jorge Timón. Freimarkets. `https://github.com/jtimon/freimarkets`, 2013. Accessed: 2018-07-24.

[6] Fernando Nieto. Trust-minimized derivatives. `https://gist.github.com/fernandonm/75cf0b0381ed92404e8a651dd790f75d`, 2018. Accessed: 2018-07-24.

[7] Joseph Poon and Thaddeus Dryja. The bitcoin lightning network: Scalable off-chain instant payments. January 14, 2016.

Appendix: Contract Diagrams

This section contains example diagrams for the contracts described in sections 3 and 4. The diagrams are styled after the LN paper[7], with some differences. Boxes correspond to transactions; the fill color indicates which blockchain the transaction takes place on, while the border color indicates who can publish the transaction. The vertical order of the boxes loosely correspond to the temporal sequence of events. The numbers should of course not be taken literally; in particular, 1 timestep should be interpreted as a quantity that allows parties to comfortably respond to their counterparty's actions in the appropriate manner.

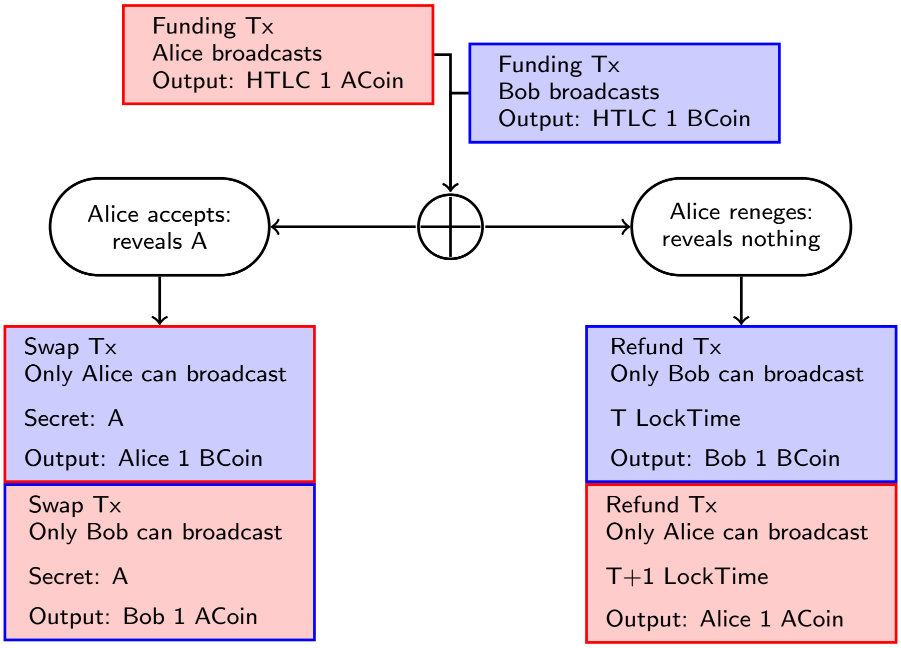


Figure 3: Atomic swap.

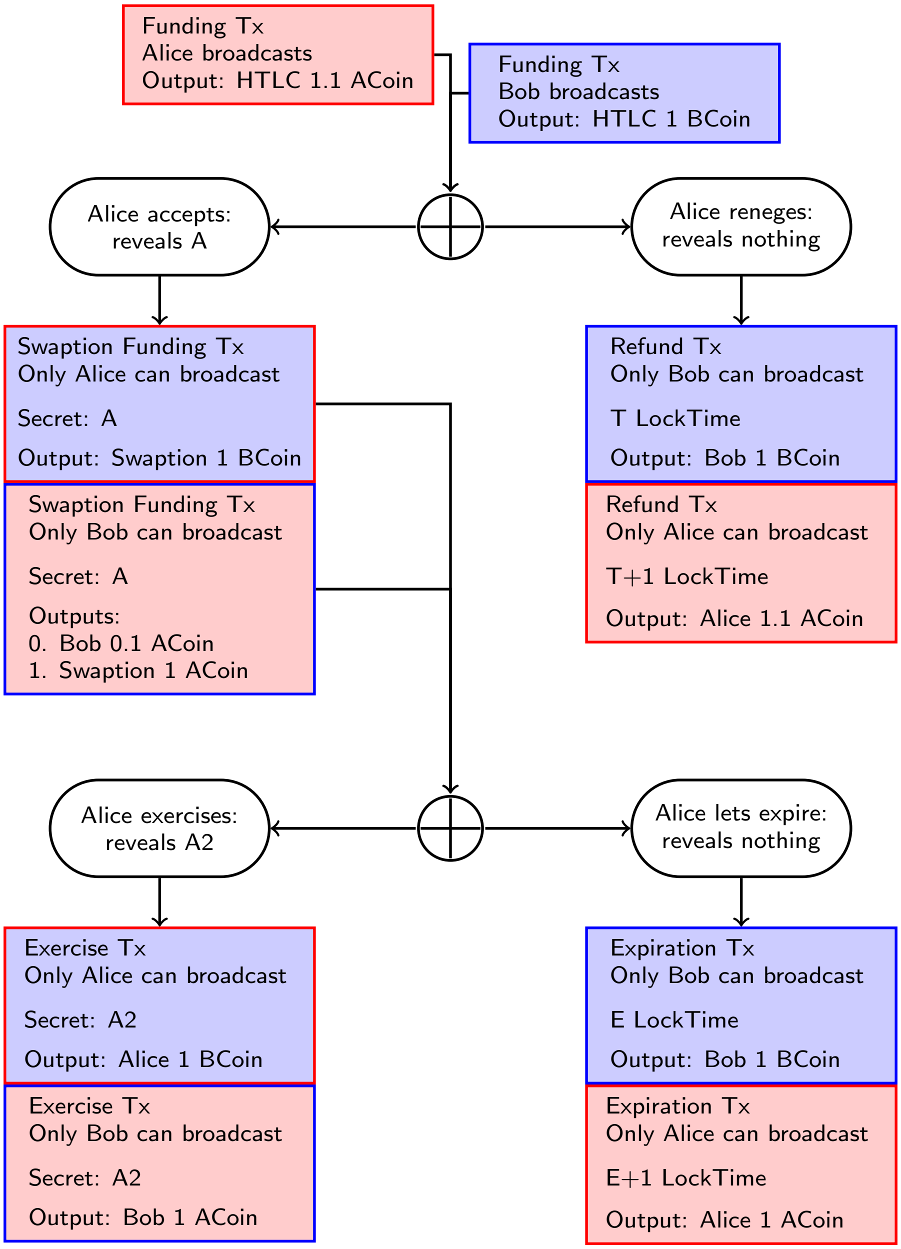


Figure 4: Basic atomic swaption construction.

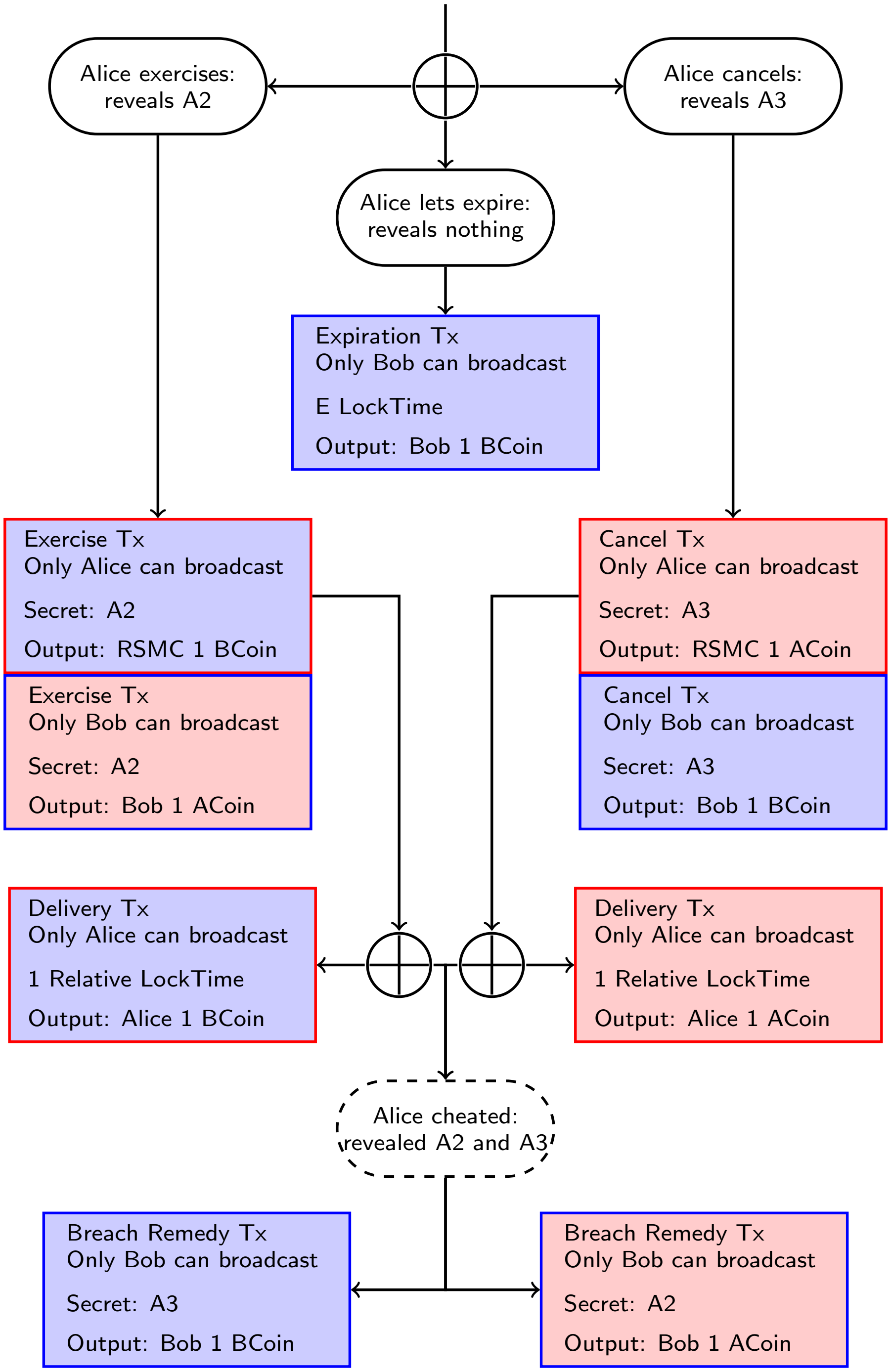


Figure 5: Early Cancellation. Unchanged portions have been omitted. Note the race conditions between Alice and Bobs' exercise and cancel transactions in the case where Alice broadcasts both transactions, which necessitates the RSMCs.

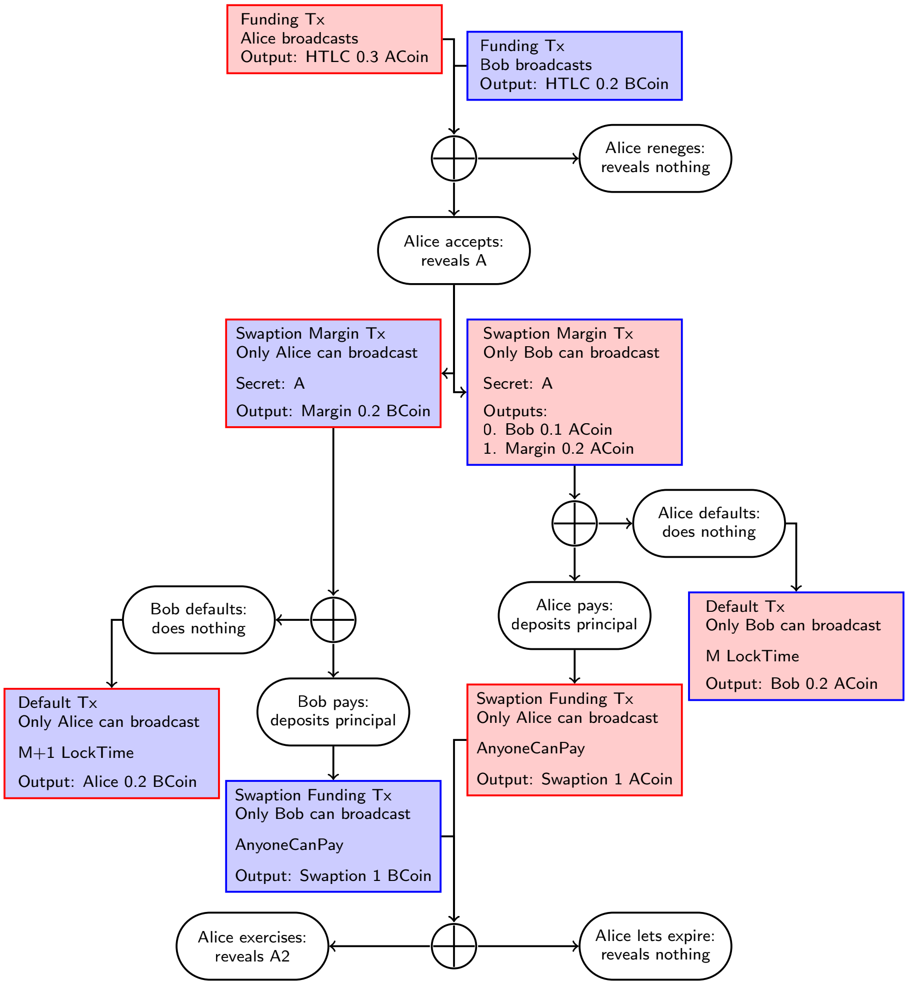


Figure 6: Swaption with margin.