Decentralized Interest Rate Swap

Tuan Tran, PhD.

August 1, 2023

In this chapter, I propose a new design for interest swap. The protocol takes in variable rates from a lending protocol and fixed rates from a bond protocol. The pricing mechanism is performed via a virtual AMM.

1 Introduction

1.1 IRS in traditional finance

When borrowing money, the borrower pays interest to the lender to compensate for the use of the money. Interest rates can be fixed or variable. A fixed interest rate is determined at the time of the loan and will not change during the term of the loan, while a variable interest rate is adjusted periodically to reflect the level of market interest rates at the time of the adjustment. In practice, there are two common proxies for variable rates: either London Inter-Bank Offered Rate (LIBOR) or prime interest rate, which is the rate at which banks in the U.S. will lend money to their most favored costumers and it depends on effective Federal funds rates.

When there are both fixed rates and variable rates, those who are exposed to variable rates can hedge the interest risks by entering an interest rate swap contract. An IRS is an agreement between two parties in which each party makes periodic interest payments to the other party based on a specified principal amount. One party pays interest on a variable rate while the other party pays interest on a fixed rate. Below are some terminology related to IRS.

- The fixed interest rate is known as the swap rate.
- The two parties in the agreement are known as counterparties.
- The counterparty who agrees to pay the swap rate is called the payer.
- The counterparty who agrees to pay the variable rate is called the receiver.
- The specified principal amount is called the notional (principal) amount.
- The specified period of the swap is known as the swap term or swap tenor.
- The dates during the swap term when the exchange of payments is to occur are settlement dates.
- The time between settlement dates is known as the settlement period.

- At payment times, the two payments are netted and only one payment is made, which is known as net swap payment.

A typical IRS contract will involve a fixed leg and a floating leg which is equal to an interest index plus a spread. For example.

$$\textbf{Fixed rate} = \textbf{LIBOR} + \textbf{Spread}.$$

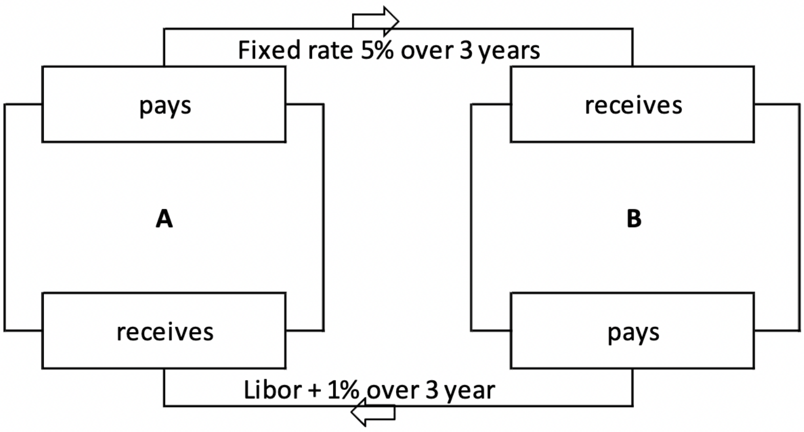

Figure 1: A typical IRS contract

Swap rate calculation. Assume that spread is zero. Let us denote by R the swap rate which is fixed, and $r_t := r_{[0,t]}$ the spot rate for the period $[0, t]$. This spot rate can be calculated from Bond prices:

$$P_t := P(0,t) = (1 + r_t)^{-t}.$$

The forward rate $f_{[t_1,t_2]}$ is defined by expected interest rate during the period $[t_1, t_2]$ and satisfies the equation

$$(1 + r_{t_2})^{t_2} = (1 + r_{t_1})^{t_1}(1 + f_{[t_1,t_2]})^{t_2-t_1}.$$

The swap rate is solution to the following equation

$$R[\Sigma_{i=1}^n P_{t_i}] = \Sigma_{i=1}^n f_{[t_i,t_{i+1}]} P_{t_i}.$$

Which implies

$$R = \frac{\Sigma_{i=1}^n f_{[t_i,t_{i+1}]} P_{t_i}}{\Sigma_{i=1}^n P_{t_i}} = \frac{1 - P_{t_n}}{\Sigma_{i=1}^n P_{t_i}}.$$

1.2 IRS on blockchain

There are several IRS protocols on blockchain, for example Voltz Finance and RabbitX (previously Strips Finance, but they changed the name after the price manipulation detection). The general way how these IRS protocol work is as follows.

- There are two types of tokens: fixed rate tokens and variable rate tokens in a given IRS pool. Variable rates are tracked from outside sources such as AAVE, Compound. Fixed rates are priced via an AMM.
- The pricing mechanism is given by a virtual AMM, i.e. it does not need LPs.
- Users deposit collateral on the platform in order to trade fixed rate tokens against variable rate tokens or vice versa.
- There is no maturity, so users can exit the contract any time.
- Funding rate $r_{var} - r_{fix}$ is settled periodically.
- Users can trade up to 10x-15x leverage. If the PnL falls below 5% of the collateral value then liquidators can liquidate the position.

To be continued.

2 A new IRS model

2.1 Pricing

We now present a new design for IRS market. Figure 2 sketches schematically the three basic components of the IRS protocol (I ignore insurance pool and liquidators to focus on the financial picture only). They include: variable leg, fixed leg, and IRS AMM. The variable rates are exogenous and imported to the IRS protocol from a lending protocol. Usually, the fixed leg will be priced via an AMM. However, in this model, the fixed rate will be imported from our own bond protocol, and the virtual AMM only focuses on pricing the premium in the equation

$$\textbf{fixed rate} = \textbf{variable rate} + \textbf{premium}.$$

The equal sign here means that the fixed rate receiver will receive the fixed rates given by the bond protocol and pay the variable rates from AAVE plus a fixed premium to the fixed rate taker.

The variable rates, fixed rates and the premium pricing AMM will be presented in the next subsections. We know focus on the modelling part.

There will be three types of IRS in our product:

- No maturity (perpetual I. This is similar to Voltz protocol. Users enter and exit anytime. The funding rates at time t are netted and settled periodically via the equation

  $$\textbf{(net swap payment)(t)} = \textbf{(fixed -premium)(0)-var (t)}$$

  At the end of a payment period, if one of the two side decides to exit the contract, then no more payment is needed.
- Fixed maturity. Assume that maturity is T but one counterparty decides to exit the contract prematurely at time $t < T$ (which we assume to be at the end of a payment period for simplicity). Other than the funding rates that have been paid up to the time t, the residual value of the contract

still needs to be settled. Assume that the premium changes from p_0 to $p_t := p_0 + \Delta p$, and the fixed rate changes from R_0^F to $R_t^F = R_0^F + \Delta R^F$ then the fixed rate payer will have to pay to the fixed rate taker an amount equal to the net present value of the residual value of the contract.

$$\textbf{residual payment} = (\Delta p - \Delta R^F)\Sigma_{s=t+1}^{T}(1 + r_t^F)^{-(s-t)},$$

where r_t^F denotes the fixed rate determined at time t. Time convention we use here is, one unit of time is equal to one settlement period.

- Infinite maturity (perpetual bond). Perpetual bonds are bonds that never pay principal but pay fixed coupons in perpetuity. The price of a perp bond that pays continuous *cdt* with discount rate R (usually is chosen to be long term bond rate, e.g. 30-year bond rate) is

  $$P = \frac{c}{R}.$$

  The formula implies that if the fixed rate changes from R_1 to R_2, then the ROI of bond buyer's investment is $R_1/R_2 - 1$. Hence, we can view the perp bond as a special tokenization of inverse interest rate $1/R$.

  We now translate this idea into an IRS with infinite maturity. In fact, the mechanism works exactly like a fixed term IRS. The only thing that differs is the way that residual value is calculated at the time that a counterparty decides to exit the contract. As maturity is perpetuity, the residual value of the contract will be

  $$\textbf{residual payment} = \frac{\Delta p - \Delta R^F}{R_t^F}.$$

2.2 Floating leg: lending protocol

The lending protocol is exogenous and follows pooling model proposed by AAVE and Compound Finance. In this model, the borrowing interest rate is designed as an increasing, deterministic function of the capital utilization ratio, which reflects the supply and demand of the capital market. Recall that,

$$r_t^B = F(U_t) = F(\frac{B_t}{L_t}),$$

where B and L denote the total borrowing and lending volume of the pool at time t. If fees are ignored, then the conservation equation below that links lending and borrowing rates should satisfy all the time:

$$r_t^L = U_t r^B t,$$

In theory, when users participate into a lending pool as a lender or a borrower, they will receive a token to recognize their deposit (for lender) or loan (for borrower). Let's call them lending notes and borrowing notes. Lending notes can be redeemed for money, and borrowing notes have to be burnt when borrowers make a payment. In principle, our IRS protocol can accept both these types of tokens: lending notes can be exchanged for bonds (as assets) and borrowing

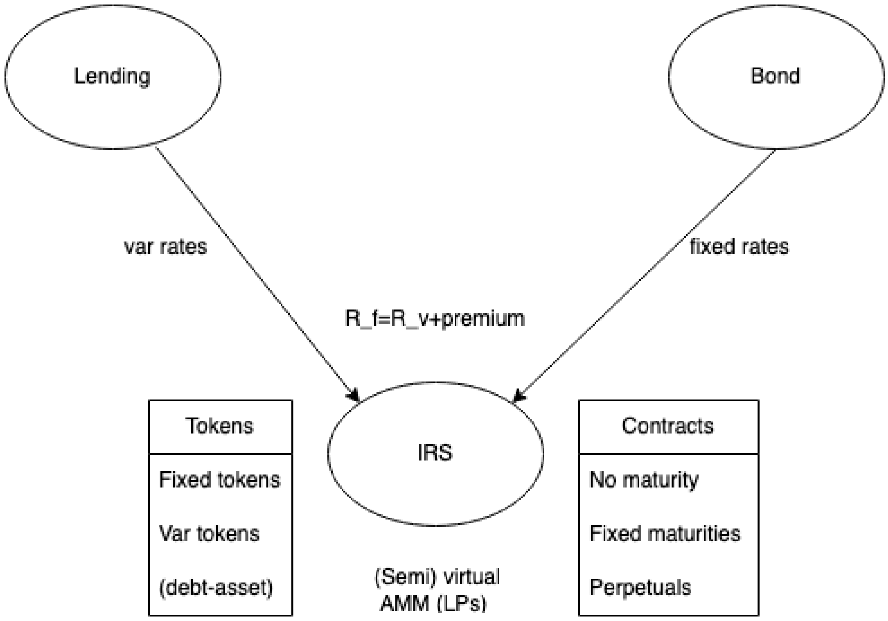

Figure 2: New IRS model

notes can be exchanged for the **bond's opposite position** (as liabilities) in swap contracts. Borrowing notes swap can be useful for borrowers when they want to hedge their loans. However, for borrowing notes, they **require further collateral** and that can complicate the swap process, so this needs more thoughts. For now, we assume we use only bonds and lending notes to exchange each other.

2.3 Fixed leg: bond AMM

Bond protocol provides fixed rates to the IRS protocol. A bond is a token that allows the buyer the right to redeem it at maturity for one DAI. The price of a bond with time-to-maturity t and implied interest rate r is given by the formulae $P = e^{-rt}$. It is important to stress that, in this bond protocol, bonds can be bought, sold, mint (short), and burnt (early payment) by users. Buying and selling activities are performed just like normal tokens. As for minting, a borrower has to stake their collateral and there will be a mechanism that estimates how much she can mint at maximum. Borrower can wait until the maturity is due and pay off their loan (if she fails to pay the loan then her collateral will be liquidated), or she can burn, whole or partially, the loan before maturity by buying back the same amount or just a part of bonds she issued and then burn them (this is equivalent to buying back the bonds and hold it until maturity, take the pay-off from the bond and then pay back the loan to the protocol, but burning just helps simplifying the whole process).

Let us consider a simplified version of the bond protocol without bid ask spread. The state space of the model is a triplet (x, y, r). More precisely.

- x denotes the amount of bonds, $x = (x_1, .., x_n)$ is a vector of bonds with different maturities $T_1, .., T_n$.
- y denotes the amount of asset (DAI) in the pool. As 1 DAI is worth roughly 1 USD, the total value at time t is $Y_t = y$.
- r denotes the reference interest rate. The net present value (NPV) of all bonds in the pool with reference rate r_t at time t is given by

$$X_t = \Sigma_{i=1}^n x_i e^{-r_t(T_i - t)}, t < T_1.$$

Reference rate. For simplicity, we assume that the reference rate is just a deterministic function of the bond proportion:

$$r = R(p), p = \frac{X}{X+Y} \in [0,1].$$

This function should be non-decreasing to reflect the fact that more bond sellers will cause bonds to be more expensive, or rates to be low. A natural choice for R is a linear function:

$$R(p) = r_{\min} + (r_{max} - r_{min})p.$$

When $p = 0, r = r_{min}$ and when $p = 1, r = r_{\max}$.

Slippage. Unlike the case of an AMM, our model requires to solve a system of partial differential equations (PDE) in general case. If the transaction relates to only one maturity, then we only have to solve an ODE of one variable.

At time t, the fixed point equation $r = R(p)$ can be rewritten as

$$r = r_{\min} + (r_{\max} - r_{\min}) \frac{\Sigma_{i=1}^n x_i e^{-r_t(T_i - t)}}{\Sigma_{i=1}^n x_i e^{-r_t(T_i - t)} + y} = F(r, x, y),$$

and

$$y = \frac{r_t - r_{\min}}{r_{\max} - r_t} \Sigma_{i=1}^n x_i e^{-r_t(T_i - t)} = G(x, r).$$

The spot price of a bond with respect to maturity T_i is given by

$$-\frac{dy}{dx_i} = e^{-r_t(T_i - t)} \, \forall i.$$

If a transaction includes multiple bond positions then we need to replace the above ODEs by PDEs

$$\frac{\partial y}{\partial x_i} = -e^{-r_t(T_i - t)} \, \forall i.$$

The above system of n PDEs (plus one fixed point equation) allow to solve numerically for (x, y, r) by substitution. In practice, we can combine an iterative algorithm with an finite difference method to solve for (x, y, r) simultaneously. Even if a transaction involves multiple maturities, it should not impose any challenge.

Bond model without NPV. Note that we can define the total notional value of all bonds as

$$X_t = \Sigma_{i=1}^n x_i.$$

with this definition, there are several advantages. First, calculation is much simpler because we do not have to solve the PDEs to estimate the price impact. Second, when time flies and there is no transaction, bonds do not need to be burnt to keep the rates unchanged. However, the major drawback of this method is time inconsistency. Plus, bonds of different maturities are considered identical from the bond pool, hence bonds of long maturities become much more expensive than bond of short maturities with the same transaction value. Consequently, **attacking the IRS protocol with long term bonds becomes easier**.

2.4 IRS AMM

Recall that our IRS does not price the fixed rates, but rather takes fixed rates as inputs and tries to price the premium (or spread) $S_t = R_t^F - R_t^V$. The long term limit of these quantities will satisfy a similar equation (and can be estimated from real data from AAVE and the bond protocol). $S_\infty = R_\infty^F - R_\infty^V$.

Now denote x^F, x^V the reserves of fixed tokens and variable tokens in the IRS pool, which are the total notional principle values-regardless of maturities. Note that **maturities should not be taken into account** when calculating total notional amount because variable tokens have no maturity.

How are these interest tokens minted? There are two ways. First, when a lending notes from AAVE or a bond notes from our bond protocol are deposited into the IRS protocol, the protocol will mint an amount of interest rate tokens equivalent to the amount of interest rates/bonds. Second, if we use a virtual AMM, then users will have to deposit their collateral assets into a separate pool and then interest tokens will be minted for them.

We want to define a bonding curve in such a way that

$$S = G(p), p = \frac{x^F}{x^F + x^V}.$$

The function G should satisfy the following conditions.

- Long term limit $p_\infty = G(0.5)$.
- Deviation: $G(0) = G(0.5) - \kappa\sigma(S), G(1) = G(0.5) + \kappa\sigma(S)$ for some constant $\kappa > 0$ (typically $\kappa = 2$), where $\sigma(S)$ denotes the standard deviation of the spread (S_t) that can be estimated from real data.

The simplest example of the pricing function G is linear function.

Remarks.

- Note that the above bonding curve model is not an AMM because it takes in exogenous price oracles R^F, R^V, therefore it needs LPs to provide liquidity.
- If we want to build a virtual AMM, then the AMM will price the fixed rate directly via the reserves instead of pricing the premium/spread (see Voltz Protocol). In this case, the bond protocol is totally independent from the IRS protocol, and to calculate the net present value of residual contract, we will use the swap rate instead of the bond yield.

2.5 Price manipulation

For IRS with infinite maturity, their price is inversely proportional to the fixed interest rate, i.e. it is extremely sensitive to the rate. A malicious agent can exploit this to attack the protocol as follows. First step, she makes a huge transaction on the bond protocol, for instance, she can sell a large amount of bond of long maturities to push the interest rates higher. Second step, she enters a long position on fixed rate IRS. Third step, she weight for the interest rate to converge to the normal level to exit the IRS position with a huge gain (while the interest rates that she paid for minting bonds are not that large if the event does not last long).

To avoid this kind of attack, we can use smoothing technique on interest rates: for interest rates of long maturities, we use longer time window to smoothen the rates. Smoothen rates tend to change slowly, hence it is hard to attack the IRS protocol simply by price manipulation on the bond protocol.