A Peer-To-Peer Bond Auction System
Using Confidence Chains

author: Joshua Zeidner
jmzeidner@gmail.com

11/2/2013

ABSTRACT

Bond auctions are an elementary component of most modern capitalistic economies. In this paper we will describe a peer-to-peer bond auction system meaning that the system 1) has no central point of failure 2) auction events are determined by a unique combination of chronology and democratic consensus that is typical to Confidence Chains based applications[1]. The system is modeled on the common Dutch Auction format[3]. Support for two bond types are described: Zero Coupon and Fixed Rate Bonds. A fully usable system would require feature basis described in [2]. This basic system provides the necessary basis to construct other useful and attractive features such as interest bearing savings accounts, personal lines of credit, community fundraising (eg. Kickstarter), and other advanced applications.

Introduction

In this paper we will describe a system of credit issuance via bond auction. This system resembles real-life financial debt brokering and is suitable for real world applications. This basic mechanism can also provide a basis for other familiar financial devices, such as interest bearing savings accounts. The system is decentralized, or peer-to-peer and has the characteristics familiar to other systems built using the Confidence Chains algorithm, namely 1) no central point of failure 2) a democratic consensus model that determines timing judgements critical to market non-bias. These systems build on top of the features described in [2]. It would behoove the reader to familiarize themselves with both [1] and [2].

An Abstract Asset Type

In an earlier work[2] a system is described for the creation and marketing of asset types. We make clear here that in our system, bond issues qualify as asset types and behave exactly as other asset types in the system. Thus they can be exchanged, traded, retailed, auctioned, and even used as payment as is possible with every other asset type. Thus it qualifies as a kind of *Object Oriented Polymorphism*, and bonds can even be embedded in other bonds(ie. bonds pay out with other bonds).

Bond Types

The system supports two common bond types: 1) Zero-Coupon Bonds and 2) Fixed Rate Bonds. A **Zero-Coupon Bond**(ZCB) is the simplest type of bond, it offers a single payment upon maturation at a fixed amount[4]. A **Fixed Rate Bond**(FRB) offers several payments(or coupons) over time at a fixed rate and pre-set interval[5]. In our system we will simplify the structure by expressing Zero-Coupon bonds as a FRB where the interval equals the expiration date(has zero coupons).

Dutch Auction

A Dutch Auction is a type of auction first developed to sell tulip bulbs in Holland[6]. It is widely thought to be an efficient and timely way to discover the price of an asset. It works as follows: 1) the auctioneer posts a quantity of some asset for sale 2) she declares some starting price(typically prohibitive) 3) buyers bid on the called price 4) the auctioneer continues to lower the price until all the assets are bid on. The result is that all the assets are sold at the lowest bid price.

ex. We have 1000 black tulip bulbs for sale

Auctioneer starts the bidding at 10 USD.
Bob bids 100 for 10 each.
Auctioneer bids 9 USD

Sally bids 500 for 9 each.
Auctioneer bids 8 USD
Rick bids 400 for 8 each.
Auctioneer declares the auction complete(price is 8 USD).

Bob buys 100 for 800 USD. (100 X $8)
Sally buys 500 for 4500 USD. (500 X $8)
Rick buys 400 for 3200 USD. (400 X $8)

In our system we abbreviate this process by simply setting a minimum price, and calling for all bids. Those bids are then lined up from highest to lowest, and those highest bids which clear out the sale are committed at the price of the lowest in the set.

Detailed System Description

Here we will describe the basic functional components of our bond market.

1. Issuing a Bond

To issue a bond a debtor specifies the expiration date, the coupon interval(how often is the debtor obligated to pay), number of coupons(how many times is the debtor obligated to pay), links a contract outlining payment terms, etc. The issue also specifies the initial recipients(which is typically the issuer).

Zero Coupon Bonds are simply a Fixed Rate Bond with no coupons. Ie. Debtor wants to issue a ZCB that matures in one year, thus the expiration date is one year from present, the interval is one year from present, and number of coupons is zero.

2. Auctioning the Bond

In our Dutch Auction, we simplify the process by posting the asset group for sale, a minimum price, and an expiration time.

3. Bidding on a Bond

Bids are made on the Bond Asset in any order, the bid must abide by the price minimum and they must be executed before the expiration time.

When the expiration time is reached, the bids are all put in order by price and the top bids that fully consume the sale product are selected, and the lowest price from that set becomes the sale price. The difference between the bid and the result price is refunded to the bidders.

4. Remarketing the Bond

The Bond can be resold or transferred in the same way any other asset can be transferred or exchanged[2].

5. Bond Transfers and Remittance

The debtor is obligated to execute remittances to the current owner of the bond at the specified intervals.

6. Default

If the debtor fails to remit funds according to the defined obligations, they are potentially in default. Typically the owner of the debt will issue a notice of default. It is included in the ledger at the discretion of the notarizing council(the identity nodes[1]).

System Details

Here we describe the structure of the Confidence Chains transactions. For more details on how these transactions appear in the confidence chain refer to [1]. Signature operations use Elliptic Curve Cryptography and hash operations use SHA256(as per Bitcoin conventions). It's recommended to be familiar with Bitcoin methodologies and conventions to grasp the meaning of the transaction description below. Each of these transaction types has a name, a description, and a set of fields.

FIXED_RATE_BOND_ISSUE

The issue of a Fixed Rate Bond(also used for Zero Coupon Bonds).

tx_id : *transaction ID*
asset_id : *the asset id class*
issuer_address : *the EC public key address of the debtor*
issued_quantity : *total quantity of issue*
issued_denominations : *smallest denomination of ownership*
creation_unixtime : *time of issue in unix time*
interval_unixtime : *intervals of remittance in unix time*
expiration_unixtime : *expiration in unix time*
remittance_asset_type : *the type of asset to be paid*
remittance_asset_value : *the amount of asset to paid*
ricardian_contract_hash : *a hash of the public contact*
ricardian_contract_url : *a url to the public contract*

issuer_sig : *a EC signature of the last 9 fields(concatenated)*
asset_outputs : *recipient accounts for the bond assets*

FIXED_RATE_REMIT

A payment on a debt obligation. Its the debtor's obligation to track the owners of the bond in the block chain. The maximum number of remittance txs required are a function of number of intervals and denomination(defined in the issue tx).

tx_id : *transaction ID*
fixed_rate_bond_issue_tx : *the transaction of the bond issue*
remittance_asset_type : *the asset type of the payment*
num_coupon : *the number of the coupon(interval)*
remit_unixtime : *time of the payment in unixtime*
remit_inputs : *funds inputs*
remit_outputs : *funds outputs*
input_sigs : *signature of inputs*

FIXED_RATE_DEFAULT

A declaration that the bond is in default.

tx_id : *transaction ID*
fixed_rate_bond_issue_tx : *the transaction of the bond issue*
default_unixtime : *the time of default in unixtime*
author_sig : *the address of the party declaring the default. The more credible the author the more weight the default declaration carries.*

FIXED_RATE_SHRED

For disposing of a bond. Must be the owner of the bond. Useful for non-marketable debt and other scenarios where the owner wishes to cancel the debt obligations owed to them.

tx_id : *transaction ID*
fixed_rate_bond_issue_tx : *the transaction of the bond issue*
shred_unixtime : *the time of disposal in unixtime*
inputs : *the inputs for the bonds to be shredded*

inputs_sig : *signature of bond inputs*

DUTCH_AUCTION_OPEN

Declares the assets up for auction(defining inputs), the price asset type, minimum price, expiration time, owner. Can be used for any asset(not only bonds).

tx_id : *transaction ID*
sale_asset_type : *asset type up for auction*
sale_inputs : *the inputs for the sale items*
minimum_price : *minimum bid price*
minimum_quantity : *minimum bid quantity*
price_asset_type : *the asset type accepted as tender for the sale item*
auction_begin_unixtime : *auction start in unixtime*
auction_expire_unixtime : *auction end in unixtime(bids must come between begin and end)*
owner_address : *the address of the auctioneer*
owner_sig : *signature of last 7 fields*
input_sigs : *signature for sale item inputs*

DUTCH_AUCTION_BID

Place a bid on a price for a given amount, set inputs, the difference between the bid and the final price is refunded in the Close tx.

tx_id : *transaction ID*
dutch_auction_tx_id : *the tx of the auction*
bid_unixtime : *time of bid in unixtime*
price : *the bid price*
quantity : *the bid quantity*
bid_asset_type : *the asset type of bid*
inputs : *inputs totalling bid price*
input sigs : *signatures for inputs*

DUTCH_AUCTION_CLOSE

Close the auction, set outputs for sold assets, refund price differences, sign off inputs.

tx_id : *transaction ID*

dutch_auction_tx_id : *the tx of the auction*
close_unixtime : *time of close in unixtime*
final_price : *final auction price per unit*
owner_sig : *signature on complete tx of auction*
refund_outputs : *outputs of the differences between winning bids and final price(necessary?)*
asset_outputs : *these are the outputs for winning bids*

Applications

Interest Bearing Savings Accounts

An interest bearing savings account is a basic feature found in most modern capitalistic environments. Such an feature can be easily derived from our bond auction system. A savings account provides these functions:

1. *deposit funds*

This is accomplished by purchasing a low-yield low-risk FRB. The interest(remittance) is automatically deposited at the owners address. Eventually the FRB expires and the interest rate must be renegotiated by a subsequent purchase of a new FRB security.

2. *withdraw funds*

This is done by remarketing the bond for a more spendable asset(eg. sell the bond for USD). Financial firms can make their products more attractive by creating automated bots for their debt instruments and offering locked in buy back rates. Thus for the type of bond used for saving accounts, it should be easy to liquidate. In most cases, the bonds will sell at a slight penalty.

The buying and selling of bonds may appear to be too much overhead for the average user, but in this new environment of crypto-finance, these complexities can be shielded from the user. These devices offer some clear advantages over traditional savings accounts eg. enhanced choice in where your money resides. Local Microcredit unions can be formed with low-barrier to entry. Third parties can develop products that are specialized for these particular purposes. For savings account, you want a very broad diverse basis of investment growth. Disruptions and defaults would be viewed as unacceptable in these use scenarios.

Simple Personal Credit Card

A Credit Card system works in precisely the reverse to that of a savings. To use a line of credit, the user either auctions or retails a bond where they hold the debt obligation. Regular remittance

transactions are required in order to avoid default. For the user to clear out their debt, they offer to buy back the bond asset at a marketable rate, then shred it. Again, most of these operations would be hidden from the end user behind more familiar controls, ie. charge, make payment, pay in full. Naturally, to have a full-fledged personal credit system there must be some notion of creditworthiness based on history or other characteristics. This can of course be derived from the record of defaults(or lack thereof) or even other factors such as social network membership. Third parties have a clear incentive to identify attractive markets for credit risk and to automate the purchase and sale of that risk for profit.

Advanced Applications

Local Co-Op Bond Tender Fundraising

Downtown Phoenix has many residents who appreciate affordable organic food, however there are no good delicatessens there. No entrepreneurs are willing to take the risk to open a place even though residents consistently complain about lack of eating venus. The solution is to organize, state the goals of the co-op, then auction ZCBs to the general public. Real capital is raised this way, basic equipment and stock is purchased, and a building is rented. There is one added twist, the ZCBs can also be used to purchase food at the deli. In addition they are also used to pay part of the employees salary, and local organic farms agree to accept them for partial payment for their goods. In this way we have raised our own funds by generating community capital that is useful and appropriate to our local social needs. Local residents now not only have a community meeting place, a great place to buy lunch, but are even invested in the success of the enterprise.

In traditional financial scenarios, it is not practical to have bonds as cash tender. In our scenario, its easy to automate the transfer of bond obligations instantly. There is demand on the part of the bond issuer to retrieve their issued debt as it nullifies debt obligations. The bond assets have a compounded local appeal, they yield real returns as would any bond plus they act as a kind of redeemable coupon for goods and services at the local business. Both parties benefit, and it begins to dissolve the barrier between business owners and patrons creating a true community cooperative scenario. The patrons are the investors. Jobs are created and services are provided with minimal real capital. Of course this application would require a relatively simple POS system that allows users to pay for goods using these alternative cash tender types. Its relatively inexpensive to support these functions with modern ‘smart’ cell phones.

Conclusion

Bond issuance and price discovery via auction provide all the basic elementary tools to create a capital rich economic environment. Confidence Chains allows for new types of usage patterns not possible with traditional bond instruments. These basic functions can provide the basis for many very useful, valuable, and profitable applications such as fundraising, savings accounts, and lines of credit. This methodology requires only a typical internet connection to host notary nodes[1], commodity

hardware, and basic application software.

References

[1] confidence chains paper
https://docs.google.com/file/d/0BwUFHE6KYsM0ZkxLVmFwbXQ3ck0/edit?usp=sharing

[2]
https://docs.google.com/document/d/1cKlN55wX7n0SLvxidLoFVrJnNMJO-Iefr8bVyeHBseg/edit?usp=sharing

[3] Dutch Auction(Investopedia.com) http://www.investopedia.com/terms/d/dutchauction.asp

[4] Zero Coupon Bond(Investopedia.com) http://www.investopedia.com/terms/z/zero-couponbond.asp

[5] Fixed Rate Bond(Investopedia.com): http://www.investopedia.com/terms/f/fixedrate-bond.asp

[6] Dutch Auction : http://www.investorwords.com/1603/Dutch_auction.html