Circular Multilateral Barter

Description:	Software design document for a novel system of trading
Author:	Evgeni Pandurksi
Contact:	epandurski@gmail.com
Date:	2009-07-12
Version:	1.1
Copyright:	This document has been placed in the public domain.

Contents

The idea in brief

In this document we propose a novel system for trading of goods which we call “Circular Multilateral Barter” (CMB). The following diagram illustrates the idea at a glance:

```
                     rice                      apples
/--->  Alice  ------------------>  Bob  ------------------->  Carl  ---\
|                                                                      |
|                                                                      |
|                                                                      |
|                                 plums                                |
\----------------------------------------------------------------------/
```

The problem

There is one very simple problem hindering trade more than anything else:

> *When traders deliver goods to buyers, they must somehow obtain trustworthy guarantees for repayment.*

The problem is so obvious that it remains largely unspoken. Nevertheless there are several quite well-known approaches for solving it:

Barter: The seller instantly obtains goods of equivalent value from the buyer.

Although ideal in some ways when it can be arranged, this method is limited to situations where a double coincidence of wants occurs.

Commodity money: The seller obtains an equivalent amount of some globally scarce good (such as gold). The seller is confident that she will be able to exchange it for something else in future as long as that good is in short supply globally.

This approach limits the amount of goods that traders are able to exchange since the amount of globally scarce goods is limited. Another disadvantage is that the good's natural value is distorted, leading to inefficiencies of use, and its value can also be manipulated by cornering the market, giving unfair advantages to some while others pay the costs.

Fiat money: The seller obtains a specific type of globally scarce good: money. The principal difference here compared to commodity money is that the money supply can be manipulated by dedicated authorities.

With the use of fiat money trading should be, at least in theory, less limited by money scarcity than it is with commodity money. Unfortunately in practice this is not always the case. Another practical problem with this approach is that the value of money becomes even more susceptible to manipulation.

The sustainable solution

In a circular transaction every seller is a buyer too. Therefore the seller instantly obtains guarantees for repayment from a trusted supplier (assuming that traders choose suppliers they trust). Normally suppliers of goods have to trust their recipients in order to be repaid. CMB effectively reverses the direction of trust, making the use of money as a medium of exchange unnecessary. CMB's approach has three principal advantages compared to other means of trading:

- CMB does not suffer the double coincidence of wants problem. The trader you deliver goods to and the trader you obtain what you need from do not need to be the same person, so there is much more flexibility for arranging trades.

- In CMB, trading is not limited by the global scarcity of any good.

- CMB uses money solely as a standard of value for a short period of time (typically a day). Thus CMB is insusceptible to changes in the value of money.

The obvious disadvantage of CMB is that the process of arranging circular transactions (waiting for a multiple coincidence of wants to occur) requires time. We believe often the advantages of CMB will make it worthwhile in spite of such delays.

How it works

The whole trading process is quite straightforward. When a buyer and a seller agree to trade a certain amount of a product at a given price, they register their agreement into a central database (see The coordinating system). Overnight the database is analyzed and a list is issued of circular transactions that are discovered. The traders themselves are responsible for the actual carrying out of the transactions[1].

The coordinating system

The coordinating system (or simply *coordinator*) is a computer system that organizes traders to engage in circular transactions. The coordinator does so by executing trading turns on a regular basis. The coordinator may decide to execute trading turns during periods of weak trading activity in order to allow traders to put their goods in other markets also.

Running a coordinating system is a serious responsibility that must be appointed to trustworthy individuals or organizations. The coordinator's software must digitally sign all documents it issues so that traders can verify the contents indisputably. Strong computer security is needed.

Trading turns

A *Trading turn* is a successive completion of the following tasks:

1. Collecting delivery agreements from traders.
2. Building a directed graph representing collected delivery agreements[2] and analyzing it to discover cycles (circular transactions).
3. Issuing a trading report containing circular transactions that are found.

Trading turns should be announced beforehand by publishing a digitally signed document, constructed in accordance with a particular regular language grammar, containing the following information:

- *turn ID*

  An unique identifier for the trading turn.

- *collection starting time*

  The time at which the collection of delivery agreements begins.

- *collection deadline*

  The time at which the collection of delivery agreements ends.

- *report deadline*

  The time at which the trading report is expected to be issued.

- *previous turn ID*

  The *turn ID* of the previous turn. All trading turns should be lined up in a singly-linked list with the most recent turn corresponding to the head of the list.

[1] When a buyer and seller digitally sign a delivery agreement, they are making a commitment to each other to carry out that transaction if it's included in a trading cycle issued by the coordinating system.

[2] In such a graph each trader becomes a vertex and each delivery agreement becomes a directed edge going from the seller to the buyer.

Delivery agreements

In the context of CMB, a *delivery agreement* (DA) is an agreement between two traders (buyer and seller) for the seller to deliver a certain amount of a given product or service, valued at a given price, to the buyer, under the coordinator's guidance. The price is just a measure of value; no money actually changes hands in the transaction.

Delivery agreements must be constructed in accordance with a particular regular language grammar, be digitally signed by both seller and buyer (see Delivery agreement signing protocol), and contain the following information:

- *turn ID*

  Announced by the coordinator beforehand. All circular transactions must be constituted entirely of delivery agreements having the same *turn ID*.

- *coordinator's public key*

  See public key cryptography.

- *buyer's public key* and *seller's public key*

  In CMB, traders' public keys serve as a form of identification. All traders must have generated their own cryptographic key pairs. Traders should keep their corresponding private keys in secret.

- *buyer's flow ID* and *seller's flow ID*

  Using more than one flow ID allows a trader to participate as if they are more than one different individual. This allows them flexibility to constrain which of their goods they trade for which other goods. Delivery agreements with the same public keys but different flow IDs must be treated by the coordinator as if they are referring to different traders.

- *product or service identifier*

  A string identifying the product or service to be delivered. All details concerning the content of the string are to be worked out bilaterally between the buyer and the seller. Traders may settle on a particular format to specify the price, the unit of measurement, the terms and conditions etc. of the product or service in question.

- *maximum value to deliver*

  The seller must be willing to deliver any amount from 0 up to the *maximum value to deliver*. Accordingly the buyer must be willing to receive any amount from 0 up to the value listed. All traders in the system must specify this field in the same measurement units. Those units should be decided and announced beforehand by the coordinator.

  Traders should agree on alternatives to cover any impossible fractional goods that might occur. For example: "up to $1000 of goats, but if I owe you a fraction of a goat I'll give you apples instead for that fractional goat, at the rate of 5 bushels of apples per goat."

  If two or more delivery agreements differ only in their *maximum value to deliver*, being otherwise identical, the biggest value is the one that matters (values don't sum up).

Delivery agreement signing protocol

Delivery agreements have to be digitally signed by both traders before being sent to the coordinator. Buyers and sellers may use the following simple protocol in order to generate signed agreements:

"Want to sell" request: Issued by the seller. Consists of the proposed DA's content. Optionally includes the seller's digital signature of DA's content.

Possible responses to this request are:

- *rejected* (includes rejection reason)
- *accepted* (includes buyer's digital signature of DA's content)
- *value is too big* (includes maximal acceptable value)

"Want to buy" request: Issued by the buyer. Consists of the proposed DA's content. Optionally includes the buyer's digital signature of DA's content.

Possible responses to this request are:

- *rejected* (includes rejection reason)
- *accepted* (includes seller's digital signature of DA's content)
- *value is too big* (includes maximal acceptable value)

Trading reports

The coordinating system must at the end of each trading turn issue a report describing all transactions it has issued for the turn. The entire report must be digitally signed by the coordinator's software so that it's verifiable that no changes or additions have been made. The coordinating system must provide all the means for traders to obtain those parts of the report which concern them directly.

Each trading report should consist of the following entities:

- one index document
- zero or more engagement documents
- zero or more circular transaction documents

Each of these documents should be constructed in accordance with a particular regular language grammar, be digitally signed by the coordinator's software, and refer to its corresponding turn ID.

To respect traders' privacy, the coordinator should only reveal information when there is a strong reason to do so. Trading reports may be delivered to a list of dedicated auditors to inspect them.

Index document

The index document should contain a list of public keys, referring to all traders engaged in circular transactions.

Engagement documents

Each engagement document should contain a public key referring to a trader, and a list of transaction IDs referring to all circular transactions in which the particular trader is engaged.

Circular transaction documents

Each circular transaction document describes a transaction that should be carried out by traders as long as it is in accordance with this whole specification. Circular transaction documents should contain the following information:

- a unique transaction ID
- transaction value
- a list of all participating delivery agreements, along with their content and the corresponding buyer's and seller's digital signatures, ordered according to their successive occurrence in the cycle

Resellers

A *reseller* is a trader which resells goods on behalf of other traders. Sellers may employ resellers in order to expand the circle of their potential clients. Special attention should be paid in implementations to allow traders to act as resellers.

Here is a incomplete list of activities a reseller may perform:

- Maintain a database containing information about traders and the goods they sell.
- Set a quality standard for trader's goods.
- Specify prices for traders' goods.
- Advertise traders' goods.
- Store trader's goods
- Collect fees form traders.

Credits

Catherine Woodgold: Coauthor of the idea.

This document would not be possible without her ideas and support.

Emil Katzarski: For his fresh ideas and healthy criticism.