A unified transactional model for integrating centrally issued currencies and mutual credit systems into the same software platform

3rd International Conference on Social and Complementary Currency Systems, Salvador, Brazil.

Author: Jorge Zaccaro, Playbanq

Electronics engineer and software developer from Colombia working on web technologies to make money available for everyone as an information system on top of the Internet. Interested in mobile wallets, social currencies, macroeconomics, monetary theory and monetary diversity.

Abstract

This article proposes a unified monetary and transactional model that enables the implementation of different currency systems in a uniform way, and a systems approach that defines a common set of data representations and interactions for sending and processing transaction requests. The monetary model is based on a generalization of mutual credit systems using configurable balance limits, and the transactional model is based on public key cryptography and digital signatures as proofs of consent. The systems approach makes use of open standards and web technologies in order to ensure ubiquitous accessibility and interoperability, and its treatment of money as information lays foundations for digital currency platforms to operate as messaging services over communication networks like the Internet.

Keywords: digital currencies, transactions

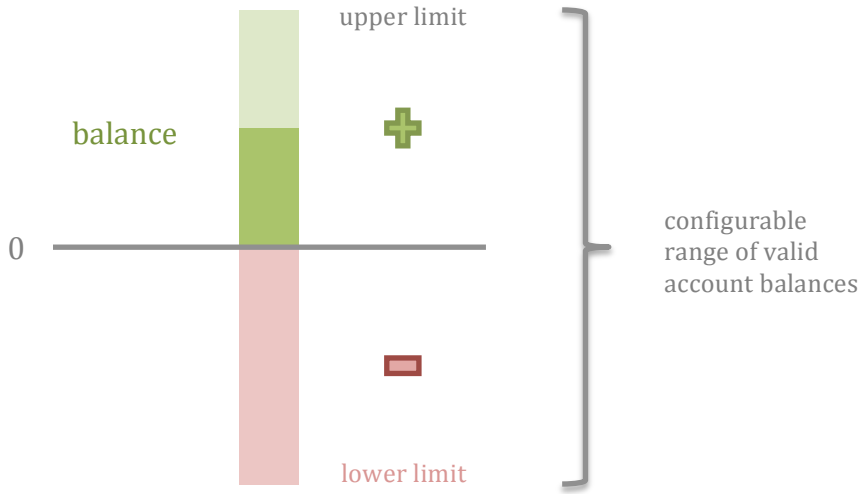
INTRODUCTION

Money is a social technology that arose from debt, not from barter, and therefore it is just information about what we owe each other. However, money is usually portrayed as a thing to be earned or borrowed, not as information that we can create ourselves, and it has not been redesigned to seize the advantages of global communication networks like the Internet. This article departs from the definition of money as information about transferable debts and builds a technical framework for any currency system to be implemented by configuring a small set of parameters and complying with a common set of constraints.

MONETARY MODEL

***Balance limits**:*

The proposed monetary model is based on the notion of configurable balance limits. Besides a balance property, each account has configurable lower and upper balance limits that are used to restrict the range of values within which the account balance must always lie. These limits can be configured to implement different currency systems such as centrally-issued currencies (only one account has a negative lower limit), cash-in currency systems (only gateway accounts have negative lower limits) and mutual credit systems (all accounts may have negative lower limits).



An account is a abstract concept used to keep count of currency units and represent payment credentials. An address is an identifier used to represent an account and reference the history of incoming and outgoing currency units. The basic representation of an account is found below:

address		string
balance		lower ≤ ≤ upper
currency		string
limits	**lower**	<= upper limit
	upper	>= lower limit

```
{
   "address": "...",
   "balance": "0",
   "currency": "...",
   "limits": {
      "lower": "0",
      "upper": null
   }
}
```

Fields used for modeling an account (left). JSON representation (right).

***Zero-sum constraints**:*

Regardless of the chosen configuration of balance limits, the resulting currency system always complies with the following constraints:

- All accounts start with a balance of zero.
- Any amount added to an account is subtracted from another account.
- The sum of all account balances is always zero.

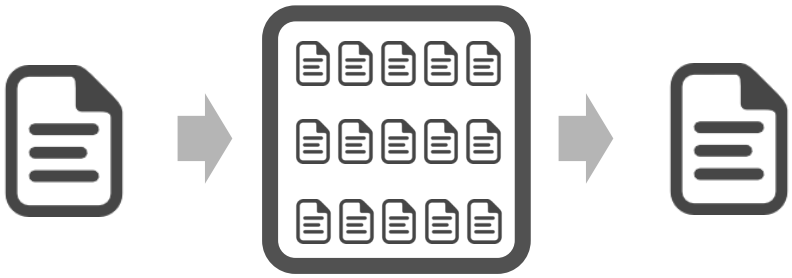
***Currency supply**:*

Given that all accounts are created with a balance of zero, every currency system must have at least one account with a negative lower limit (depicted with a red bar below), so that a currency supply (depicted with a blue bar below) can be created and eventually used by the remaining accounts (depicted with green bars below) to carry out transactions between them.

The currency supply is created, increased or decreased by sending transactions from/to accounts with negative lower limits. It can be a fixed amount issued upfront (limited assets), a growing amount increased on-demand (centrally-issued currencies), a dynamic amount changed on-demand (mutual credit systems), or any combination thereof.

TRANSACTIONAL MODEL

The proposed transactional model is based on the notion of a system that consumes cryptographically signed IOUs and serves publicly verifiable records that represent the states of accounts, while keeping the history of all balance modifications in a cryptographically secure way (transaction chains).



IOU:

An IOU is a cryptographically signed message that acknowledges a debt and authorizes the modification of the involved account balances. IOUs are the building blocks of transaction requests, and their signatures act as proofs of consent of the signing parties to participate in a transaction. IOUs are modeled using five basic parameters: the source and destination accounts, the value and currency of the transaction, and a timestamp.

header	signing key and algorithm
subject	source account
audience	destination account
value	transaction value
currency	transaction currency
timestamp	ISO date
signature	cryptographic signature

```
{
   "header": {...},
   "payload": {
      "sub": "source",
      "aud": "destination",
      "val": "number",
      "iou": "IOU:ABC123",
      "iat": "issuedAtDate"
   },
   "signature": "..."
}
```

IOUs are structured according to the JSON Web Signature specification (JWS), and the fields are named after the claims defined in the JSON Web Token specification (JWT), both open standards from the Internet Engineering Task Force.

***Transaction request**:*

A transaction request is a message that groups all information required for carrying out a transaction. Transaction request documents act as temporary stores until all input IOUs are received (instructions and account signatures) and all outputs are calculated (aggregate account balance changes).

count	incremental number
amount	transaction amount
inputs	IOUs and signatures
outputs	balance changes
timestamps	IOUs reception dates
signatures (internal validation, audits)	cryptographic signatures

```
{
   "payload": {
      "count": "source",
      "amount": "destination",
      "inputs": [...],
      "outputs": [...],
      "timestamps": [...]
   },
   "signatures": [...]
}
```

Although the number of IOUs in a transaction request and the number of signatures required per IOU is fully configurable, the following constraints must be met:

- Each transaction request must have at least one input IOU (in the "inputs" array).
- Each IOU must have at least two signatures (at least one from each listed account).
- Each transaction request must generate at least two outputs (in the "outputs" array).

***Transaction record**:*

A transaction record is a transaction request that has been processed and included in a transaction chain, along with one or more cryptographic signatures that confirm the transaction as valid. A transaction chain is a sequence of transaction records where each record is linked to the previous one by including a cryptographically secure reference to it, so that no reordering or tampering can take place without breaking the cryptographic integrity of the chain.

GLOSSARY

Money	Information about transferable debts
Debt	An obligation to complete a partial exchange
IOU (I Owe You)	A signed document that acknowledges a debt
Currency	An abstract unit of account in which debts are denominated
Currency unit	An arbitrary increment on an abstract scale of measurement
Currency system	A system that follows a set of rules to keep accounts of currency units
Currency supply	The amount of existing currency units at a particular point in time
Currency circle	A set of accounts whose balances are denominated in the same currency
Account	An entity used to keep count of incoming and outgoing currency units
Transaction	An operation that atomically transfers currency units between accounts

REFERENCES

Kennedy, M.I. & Lietaer, B.A., 2012. *People money the promise of regional currencies*, Axminster, Devon, United Kingdom: Triarchy Press.

Lietaer, B.A. & Dunne, J., 2013. *Rethinking money how new currencies turn scarcity into prosperity*, San Francisco: Berrett-Koehler.

Martin, F., 2015. *Money: the unauthorized biography from coinage to cryptocurrencies*, Vintage.

Rosenblith, A., 2009. *The Money Fix*, United States: Alan Rosenblith.