Value-Exchange-System

based on cryptography and blockchain

Carl Friedrich von Mises

29.02.2024

(AI-Translated from German)

Table Of Contents

1 General

Can people trade directly with each other? So far, this idea seems very impractical for various reasons. This document presents an idea of an exchange system in which money in the conventional sense does not necessarily have to be used.

The concept described should serve as food for thought. Several different perspectives can enrich the project.

All terms used were used freely according to the usage of the creator and do not follow any specific definition or the like. The focus is on general understanding.

2 Goal

This system is intended to achieve the following goals:

- A fair trading system that does not require the use of currencies
- Every action is based on voluntariness
- Values remain in the region
- A return to the fundamental advantages of the market economy
- Awareness of the actual creation of values
- Making external influences more difficult (interventionism)

3 Implementation

- Anyone who has a value to offer can create a certificate for it.
- A certificate contains, among other things, the quantity, the type, the place of transfer and the end date of validity. (Similar to the well-known 'bill of exchange' or 'bill of exchange')
- The issuer of the certificate can now exchange it for other certificates - a trade is created.
- Until the end date, the certificate holder has the opportunity to take possession of the real goods at the place of transfer by presenting the certificate.

3.1 Participants

Jeder Mensch kann freiwillig jede Position, und auch mehrere gleichzeitig, einnehmen. Es wird nur eine eindeutige Teilnehmer-Kennung benötigt.

3.1.1 Certificate issuer

- Has a real value (goods, gold, EUR, BTC, service, labor)
- Selects a server and software
- Creates a certificate and enters it into the exchange
- Has the obligation to hand over the value of the goods upon presentation of a valid certificate by the certificate holder.
- When creating the certificate, any server operator and software developer must be selected on their terms.

3.1.2 Certificate holder

- Holds a certificate which he has previously obtained by exchange or creation.
- Has the right to take possession of the value of the goods upon presentation of a valid certificate to the certificate issuer.

3.1.3 Server operator

- Operates a server to maintain the network.
- Receives remuneration when a certificate is created.
- He can determine the amount of the fee by himself.
- Only certificates with the correct remuneration are accepted.

3.1.4 Software developer

- Develops an application (certificate creation/trading)
- Offers the software to participants.
- Receives remuneration when a certificate is created with this software.
- He can determine the amount of the fee by himself.
- Only certificates with the correct remuneration are accepted.

4 Database

The server operators manage the data in the form of a blockchain. Several blockchains can exist in parallel. Different blockchains represent different regions. Trading between them is not possible.

There are the following database entries (schematic):

4.1 Certificate

Blockchain ID	Unique identification blockchain (marketplace)
Certificate ID	Unique identification certificate
Date	Date of creation
Creator identifier	Unique user ID
Redemption start date	Start date of redeemability
Redemption end date	End date of redeemability
Article	Description of the real value (category, quality, etc.)
Quantity	Quantity of the value
Place of transfer	Place of transfer
Server operator	Unique user ID
	Remuneration in %
Software developer	Unique user ID
	Remuneration in %
Other costs 1...n	Unique user ID
	Remuneration in %
Software signing	Signing
Server signing	Signing

4.2 Transaction - Certificate exchange

Transaction ID	Unique identification Transaction
Certificate ID	Unique identification Certificate
Date	Date of the transaction
Party A identifier	Unique user ID
Party A Certificate	ID of the exchange goods
Party A Quantity	Quantity of exchange goods
Party A Signing	Signing
Party B identifier	Unique user ID
Party B Certificate	ID of the exchange goods
Party B Quantity	Quantity of exchange goods
Party B Signing	Signing
Software signing	Signing
Server signing	Signing

4.3 Transaction - Transfer of goods

Transaction ID	Unique identification Transaction
Certificate ID	Unique identification Certificate
Date	Date of the transaction
Creator identifier	Unique user ID (encoder)
Quantity	Quantity of exchanged goods
Signing	Signature (goods handed over)
Recipient identifier	Unique user ID
Recipient signing	Signature (goods received)
Software signing	Signing
Server signing	Signing

5 Software

5.1 User software

The user software must contain the following functions:

- Creation of a participant
- Creation of a certificate
- Trading of certificates
- Signing of certificates/transactions (private key)
- Verification of certificates/transactions and transmission to the server network

Further possibilities could be:

- Portfolio of all certificates held
- Release certificate for trading
- Release only for certain counterparties, direct trading with known parties
- Limit search to a radius (e.g. 20km)
- Contact list, favorites
- Rating of participants, reviews, fraudulent transactions, trust level
- Overview of which goods are offered for my product and at what value
- Order book/volume similar to well-known trading platforms
- Different order types (market, limit, ...)
- One-cancels-the-other order if you want this or that commodity
- Connectivity to a cryptocurrency wallet

5.2 Server software

The server software must contain the following functions:

- Utilization of all created certificates and transactions
- Verification of certificates/transactions and entry in the blockchain
- Synchronization with all other servers that operate the same blockchain

All actions of the individual participants are cryptographically signed and ultimately written to the blockchain.

6 Examples

6.1 How it works in principle

A farmer has 100 kg of potatoes that he wants to bring to market.
He creates 1 certificate for 100 kg of potatoes with a validity period of 6 months (shelf life)

In the app he uses, he first stores a preferred server operator. The software creator is fixed. Both charge 1% in fees. By signing the certificate, the farmer accepts the conditions.
The app checks the correctness and sends the request to the server, which must be available and synchronized with the server network. The server checks again that everything is correct and enters the data into the blockchain. The entire server network must now synchronize with the new data.

By querying the blockchain, it is now known that the farmer holds 98% of the certificate and the server operator and software creator each hold 1%. These also appear in the portfolio section of the app.
Each certificate holder can now offer the certificate for trade in the trading area of the app. He specifies what he wants in return (potato/beef, potato/working time, potato/money). A large number of trading pairs are created. A counterparty who needs potatoes and wants to offer the desired good makes an offer. If both accept, the transaction is transmitted to the server and entered in the blockchain. The place of redemption and the expiry date will influence the agreement.

The certificates can circulate freely. If a holder of a certificate for 10 kg of potatoes comes to the farmer and wants the potato, he creates a request to hand over the goods. The farmer checks the correctness (identity, certificate) via a QR code, hands over the goods and confirms the handover of the goods in the app. The holder also confirms this and the corresponding transaction is entered in the blockchain. In the case of a transaction involving the physical handover of goods, the certificate expires according to the quantity handed over.

6.2 Delivery

A certificate holder wants to exchange a product but does not want to make the journey. He exchanges some of the certificates he holds with a delivery service, which then takes care of the transportation. Or he creates a certificate with any goods, which he instructs the delivery service with.
When collecting the physical goods from the certificate issuer, the issuer confirms the handover, and when delivering to the recipient, the recipient confirms receipt.
The recipient also confirms that the delivery service has completed the service.

6.3 Marketplace

A local retailer wants to run a store where customers can buy goods on site. He obtains all the required certificates for the products he wants to offer beforehand and has the goods physically delivered. (Purchasing)
For the goods now in his possession, he creates certificates himself, which he in turn exchanges with his customers and then hands over the goods. (Sale)

6.4 Money lending

A person needs liquidity (e.g. 1.00 BTC) in order to make a major purchase.

He creates a certificate for 1.05 BTC with a term of one year but an earliest redemption date of 10 months. He offers this certificate on the market for 1.00 BTC.
If a creditor accepts this offer and exchanges his own certificate with the debtor, the debtor can

immediately redeem 1.00 BTC in real terms.
After 10 months, the creditor demands 1.05 BTC from the debtor.

Particularly liquid goods establish themselves as a kind of currency. Particularly trustworthy participants could then act as exchangers for liquidity.
As the issuer and the term are visible for every transaction, the exchanger is forced to always act correctly.

6.5 Server-Operator/-Costs

The server costs are too high for a producer (certificate creator). He now operates his own server with a 0% fee in order to reduce the devaluation in certificate creation.
Or he charges a fee and can thus profit from other issuers.
A market equilibrium will emerge.

6.6 Software-Developer/-Costs

A software company profits enormously from the many certificates and the resulting fees. This attracts other companies and creates competition.
A market equilibrium will emerge.

7 Problems

7.1 Anonymity

The certificate creator must disclose their identity or the transfer location so that people can rely on the promise. Different users and several smaller, private blockchains could counteract this. Ideally, the identities would only be visible to the participants involved in exchange requests and trading.

It would also be conceivable for certificates to be printed out by the holder and then passed on offline. The first person to scan it would then book it in their portfolio.

7.2 Fraud / Dispute

Basically, this system is based on the trust that the promised goods will actually be delivered. But what happens if this does not happen? (Goods are not delivered or delivery of goods is not confirmed)

It is conceivable that an arbitrator could be integrated into the system to decide in the event of disagreements and misunderstandings.
But how do the parties agree on the choice of arbitrator? Since a certificate can circulate and ultimately an unknown party can also claim the genuine goods, the arbitrator would have to be appointed directly when the certificate is created. When the certificate is exchanged, the recipient then accepts the arbitrator's choice.
A separate database entry could be used for the arbitrator's judgment.

7.3 The State

It is conceivable that a state would like to take a certain percentage. If people are forced to do so, the state would still only receive a share of the certificate produced in the region (e.g. 10 kg of potatoes). The actual value would ultimately return to the region of origin.

8 Completion

It is possible that this barter system brings many advantages and is readily accepted by people. However, it could also meet with rejection and be fought against, or any weaknesses could be exploited to their advantage by disgruntled contemporaries.
Ideally, many smaller, regional systems would emerge in the spirit of decentralization.
If the concept turns out to be useless, it will disappear all by itself.

In principle, we already have a system similar to this. The only difference is that the main certificate traded is fiat money. However, this can be very easily influenced by the money supply and interest rates. In addition, the value can be transferred to other regions of the world at the touch of a button. In the system presented here, the value of all certificates generated would end up back in the region at the end of the term at the latest.

It would already be a huge step forward if people understood the current system better. What is money and how is it created? With this system, all traded goods become their own currency, so to speak, which would also provide a good basis for real currency competition.

The files can also be found here:
https://github.com/CarlFriedrichvonMises/Value-Exchange-System
https://codeberg.org/CarlFriedrichvonMises/Value-Exchange-System

MONERO

bitcoin