Werte-Tausch-System

basierend auf Kryptographie und Blockchain

Carl Friedrich von Mises

29.02.2024

(Original Version – German)

Inhaltsverzeichnis

1 Allgemeines

Können Menschen direkten Handel miteinander betreiben? Bisher scheint diese Vorstellung aus verschiedenen Gründen sehr unpraktikabel. In diesem Dokument wird eine Idee eines Tauschsystems vorgestellt, bei welchem Geld im herkömmlichen Sinne nicht unbedingt verwendet werden muss.

Das beschriebene Konzept sollte als Denkanstoß dienen. Mehrere verschiedene Perspektiven können das Projekt bereichern.

Alle verwendeten Begriffe wurden frei nach dem Sprachgebrauch des Erstellers verwendet und folgen keiner bestimmten Definition oder dergleichen. Das allgemeine Verständnis steht im Vordergrund.

2 Ziel

Folgende Ziele soll dieses System erreichen:

- Ein gerechtes Handelssystem, welches auch ohne die Verwendung von Währungen auskommt
- Jede Handlung basiert auf Freiwilligkeit
- Werte bleiben in der Region
- Rückbesinnung auf die grundsätzlichen Vorteile der Marktwirtschaft
- Bewusstsein über die eigentliche Entstehung von Werten
- Erschwerung externer Einflüsse (Interventionismus)

3 Umsetzung

- Jeder, der einen Wert anzubieten hat, kann ein Zertifikat dafür erstellen.
- Ein Zertifikat beinhaltet u.a. die Menge, die Art, den Übergabeort, sowie das Enddatum der Gültigkeit. (Ähnlich dem bekannten ‚Wechsel' oder ‚Bill of Exchange')
- Der Ersteller des Zertifikates kann dieses nun gegen andere Zertifikate eintauschen - ein Handel entsteht.
- Bis zum Enddatum hat der Zertifikat-Halter durch das Vorzeigen des Zertifikats die Möglichkeit, die reale Ware am Übergabeort in Besitz zu nehmen.

3.1 Teilnehmer

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

3.1.1 Zertifikat-Ersteller

- Besitzt einen realen Wert (Waren, Gold, EUR, BTC, Dienstleistung, Arbeit)
- Wählt einen Server und eine Software
- Erstellt ein Zertifikat und gibt es in den Tauschhandel
- Hat die Pflicht, bei Vorlage eines gültigen Zertifikates durch den Zertifikat-Halter, den Warenwert auszuhändigen.
- Beim Erstellen des Zertifikates muss ein beliebiger Server-Betreiber und ein Software-Entwickler zu deren Konditionen gewählt werden.

3.1.2 Zertifikat-Halter

- Hält ein Zertifikat, welches er zuvor durch Tausch oder Erstellung erlangt hat.
- Hat das Recht, bei Vorlage eines gültigen Zertifikates beim Zertifikat-Ersteller, den Warenwert in Besitz zu nehmen.

3.1.3 Server-Betreiber

- Betreibt einen Server, um das Netzwerk aufrecht zu erhalten.
- Bekommt eine Vergütung beim Erstellen eines Zertifikates.
- Die Höhe der Vergütung legt er selbst fest.
- Es werden nur Zertifikate mit korrekter Vergütung angenommen.

3.1.4 Software-Entwickler

- Entwickelt eine Anwendung (Zertifikat-Erstellung / -Handel)
- Er bietet die Software den Teilnehmern an.
- Bekommt eine Vergütung beim Erstellen eines Zertifikates mit dieser Software.
- Die Höhe der Vergütung legt er selbst fest.
- Es werden nur Zertifikate mit korrekter Vergütung angenommen.

4 Datenbank

Die Server-Betreiber verwalten die Daten in Form einer Blockchain. Es können mehrere Blockchains parallel existieren. Verschiedene Blockchains stellen unterschiedliche Regionen dar. Ein Handel untereinander ist nicht möglich.

Es gibt folgende Datenbank-Einträge (Schematisch):

4.1 Zertifikat

Blockchain-ID	Eindeutige Identifikation Blockchain (Marktplatz)
Zertifikat-ID	Eindeutige Identifikation Zertifikat
Datum	Datum der Erstellung
Ersteller Kennung	Eindeutige Benutzerkennung
Einlösedatum Beginn	Anfangsdatum der Einlösbarkeit
Einlösedatum Ende	Enddatum der Einlösbarkeit
Artikel	Beschreibung des realen Wertes (Kategorie, Qualität, etc.)
Anzahl	Menge des Wertes
Übergabeort	Ort der Übergabe
Server-Betreiber	Eindeutige Benutzerkennung
	Vergütung in %
Software-Entwickler	Eindeutige Benutzerkennung
	Vergütung in %
Sonstige Kosten 1...n	Eindeutige Benutzerkennung
	Vergütung in %
Software Signierung	Signierung
Server Signierung	Signierung

4.2 Transaktion Zertifikat-Tausch

Transaktions-ID	Eindeutige Identifikation Transaktion
Zertifikat-ID	Eindeutige Identifikation Zertifikat
Datum	Datum der Transaktion
Partei A Kennung	Eindeutige Benutzerkennung
Partei A Zertifikat	ID der Tauschware
Partei A Anzahl	Menge der Tauschware
Partei A Signierung	Signierung
Partei B Kennung	Eindeutige Benutzerkennung
Partei B Zertifikat	ID der Tauschware
Partei B Anzahl	Menge der Tauschware
Partei B Signierung	Signierung
Software Signierung	Signierung
Server Signierung	Signierung

4.3 Transaktion Warenübergabe

Transaktions-ID	Eindeutige Identifikation Transaktion
Zertifikat-ID	Eindeutige Identifikation Zertifikat
Datum	Datum der Transaktion
Ersteller Kennung	Eindeutige Benutzerkennung (Geber)
Anzahl	Menge der Tauschware
Signierung	Signierung (Ware ausgehändigt)
Empfänger Kennung	Eindeutige Benutzerkennung
Empfänger Signierung	Signierung (Ware erhalten)
Software Signierung	Signierung
Server Signierung	Signierung

5 Software

5.1 Anwender-Software

Die Anwender-Software muss folgende Funktionen enthalten:

- Erstellung eines Teilnehmers
- Erstellung eines Zertifikates
- Handel der Zertifikate
- Signierung der Zertifikate/Transaktionen (Privatekey)
- Überprüfung der Zertifikate/Transaktionen und Übermittlung an das Servernetzwerk

Weitere Möglichkeiten könnten sein:

- Portfolio aller gehaltenen Zertifikate
- Freigabe Zertifikat für Handel
- Freigabe nur für gewisse Gegenparteien, Direkthandel mit Bekannten
- Suche auf Umkreis beschränken (z.B. 20km)
- Kontaktliste, Favoriten
- Bewertung Teilnehmer, Rezensionen, Betrügerische Transaktionen, Vertrauenslevel
- Übersicht, welche Waren für mein Produkt zu welchem Gegenwert geboten werden
- Orderbuch/-volumen ähnlich bekannter Trading-Plattformen
- Verschiedene Ordertypen (Market, Limit, ...)
- One-Cancels-The-Other-Order, wenn man diese oder jene Ware haben möchte
- Konnektivität zu einer Kryptowährungs-Wallet

5.2 Server-Software

Die Server-Software muss folgende Funktionen enthalten:

- Verwertung aller erstellten Zertifikaten und Transaktionen
- Überprüfung der Zertifikate/Transaktionen und Eintrag in die Blockchain
- Synchronisation mit allen anderen Servern, welche dieselbe Blockchain betreiben

Alle Handlungen der einzelnen Teilnehmer werden kryptographisch signiert und letztendlich in die Blockchain geschrieben.

6 Beispiele

6.1 Prinzipielle Funktionsweise

Ein Bauer hat 100kg Kartoffel, die er auf den Markt bringen möchte.
Er erstellt 1 Zertifikat über 100kg Kartoffel mit einer Laufzeit von 6 Monaten (Haltbarkeit)

In der App, die er nutzt, hinterlegt er zuvor einen bevorzugten Server-Betreiber. Der Software-Ersteller ist fix hinterlegt. Beide fordern je 1% an Gebühren. Mit der Signierung des Zertifikates akzeptiert der Bauer die Konditionen.
Die App überprüft die Richtigkeit und sendet die Anfrage an den Server, welcher verfügbar und mit dem Server-Netzwerk synchronisiert sein muss. Der Server prüft nochmal, ob alles stimmt und trägt die Daten in die Blockchain ein. Nun muss sich gesamte Server-Netzwerk mit den neuen Daten synchronisieren.

Durch Abfrage der Blockchain weiß man nun, dass der Bauer 98% und der Server-Betreiber bzw. der Software-Ersteller je 1% des Zertifikates halten. Diese erscheinen auch im Portfolio-Bereich der App.
Jeder der Zertifikat-Halter kann nun das Zertifikat im Handels-Bereich der App zum Handel anbieten. Dabei gibt er an, was er dafür haben möchte (Kartoffel/Rindfleisch, Kartoffel/Arbeitszeit, Kartoffel/Geld). Es entsteht eine Vielzahl an Handelspaaren. Eine Gegenpartei, welche Kartoffel benötigt, und selbst das gewünschte Gut anbieten will, macht ein Angebot. Wenn beide akzeptieren, wird die Transaktion an den Server übermittelt und in die Blockchain eingetragen. Der Einlöseort und das Verfallsdatum wird dabei Einfluss auf die Einigkeit haben.

Die Zertifikate können beliebig zirkulieren. Kommt nun ein Halter eines Zertifikates in Höhe von 10kg Kartoffel zum Bauer und will die Kartoffel haben, so erstellt er eine Anforderung auf Warenübergabe. Der Bauer prüft über einen QR-Code die Richtigkeit (Identität, Zertifikat), übergibt die Ware und bestätigt in der App die Warenübergabe. Der Halter bestätigt dies ebenso und die entsprechende Transaktion wird in die Blockchain eingetragen. Bei einer Transaktion mit physischer Warenübergabe erlischt das Zertifikat entsprechend der übergebenen Menge.

6.2 Lieferung

Ein Zertifikat-Halter möchte eine Ware eintauschen, möchte aber den Weg nicht auf sich nehmen. Er tauscht einen Teil der gehaltenen Zertifikate mit einem Lieferdienst, welcher sich dann um den Transport kümmert. Oder er erstellt ein Zertifikat mit beliebigem Gut, mit dem er den Lieferdienst beauftragt.
Bei der Abholung der physischen Güter vom Zertifikat-Ersteller bestätigt dieser die Übergabe, bei der Lieferung an den Empfänger bestätigt dieser den Erhalt.
Weiters bestätigt der Empfänger die abgeschlossene Dienstleistung des Lieferservices.

6.3 Marktplatz

Ein Händler im Ort möchte ein Geschäft betreiben, wo die Kunden die Waren vor Ort erwerben können. Für die Produkte, die er anbieten will, besorgt er sich zuvor alle gewünschten Zertifikate und lässt sich die Waren physisch liefern. (Einkauf)
Für die sich nun in seinem Besitz befindlichen Waren erstellt er selbst Zertifikate, welche er wiederum mit seinen Kunden tauscht und in weiter Folge die Ware übergibt. (Verkauf)

6.4 Geldverleih

Ein Mensch benötigt Liquidität (z.B. 1,00 BTC), um eine größere Anschaffung machen zu können.

Er erstellt ein Zertifikat über 1,05 BTC mit einer Laufzeit von einem Jahr, aber einer frühesten Einlösbarkeit von 10 Monaten. Am Markt bietet er dieses Zertifikat für 1,00 BTC an.

Geht ein Gläubiger auf dieses Angebot ein und tauscht sein eigenes Zertifikat mit dem Schuldner, so kann der Schuldner sofort 1,00 BTC real einlösen.
Nach 10 Monaten fordert der Gläubiger 1.05 BTC vom Schuldner.

Besonders liquide Güter etablieren sich als eine Art Währung. Besonders vertrauenswürdige Teilnehmer könnten dann als Wechsler für Liquidität agieren.
Da bei jeder Transaktion der Herausgeber und die Laufzeit ersichtlich ist, ist der Wechsler gezwungen, stets korrekt zu handeln.

6.5 Server-Betreiber/-Kosten

Für einen Produzenten (Zertifikat-Ersteller) sind die Serverkosten zu hoch. Er betreibt nun einen eigenen Server mit 0% Gebühr, um so die Abwertung bei der Zertifikat-Erstellung zu mindern.
Oder aber er verlangt eine Gebühr und kann somit von anderen Herausgebern profitieren.
Es wird sich ein marktwirtschaftliches Gleichgewicht einstellen.

6.6 Software-Entwickler/-Kosten

Ein Softwareunternehmen profitiert enorm durch die vielen Zertifikate und die dadurch entstehenden Gebühren. Dies zieht andere Unternehmen an, es entsteht eine Konkurrenz.
Es wird sich ein marktwirtschaftliches Gleichgewicht einstellen.

7 Probleme

7.1 Anonymität

Der Zertifikat-Ersteller muss seine Identität bzw. den Übergabeort bekanntgeben, damit sich die Menschen auf das Versprechen verlassen können. Verschiedene Benutzer und mehrere kleinere, private Blockchains könnten dem entgegenwirken.
Im Idealfall wären die Identitäten nur für die beteiligten Teilnehmer bei Tausch-Anfrage und Handel ersichtlich.

Weiters wäre es auch vorstellbar, dass Zertifikate vom Halter ausgedruckt und diese dann offline weitergegeben werden. Bei jenem, der es als erstes einscannt, wird es dann im Portfolio verbucht.

7.2 Betrug / Streit

Grundsätzlich basiert dieses System auf dem Vertrauen, dass die versprochene Ware auch wirklich ausgehändigt wird. Aber was passiert, wenn dies nicht geschieht? (Ware wird nicht ausgehändigt oder Wareübergabe wird nicht bestätigt)

Es wäre vorstellbar, dass ein Schlichter, welcher im Falle von Uneinigkeit und Missverständnissen entscheidet, in das System integriert wird.
Aber wie einigen sich die Parteien auf die Wahl des Schlichters? Da ein Zertifikat zirkulieren und letztendlich auch ein Unbekannter die echte Ware einfordern kann, müsste der Schlichter direkt bei Zertifikat-Erstellung bestimmt werden. Beim Zertifikat-Tausch akzeptiert dann der Empfänger die Wahl des Schlichters.
Für das Urteil des Schlichters könnte ein eigener Datenbank-Eintrag genutzt werden.

7.3 Staat

Es ist denkbar, dass ein Staat sich einen gewissen Prozentsatz einverleiben möchte. Sollten die Menschen dazu gezwungen werden, würde der Staat trotzdem nur einen Anteil des in der Region erstellten Zertifikates bekommen (z.B. 10kg Kartoffel). Der eigentliche Wert kommt letztendlich wieder in die Ursprungsregion zurück.

8 Abschluss

Möglicherweise bringt dieses Tauschsystem viele Vorteile und wird von den Menschen gerne angenommen. Es könnte aber auch auf Ablehnung stoßen und bekämpft, oder etwaige Schwachstellen von missgünstigen Zeitgenossen zu deren Vorteil ausgenutzt werden.
Im Sinne der Dezentralität würden idealerweise viele kleinere, regionale Systeme entstehen. Sollte sich herausstellen, dass das Konzept unbrauchbar ist, so wird es von ganz allein wieder verschwinden.

Im Prinzip haben wir bereits ein so ähnliches System. Nur dass das hauptsächlich gehandelte Zertifikat das Fiat Geld ist. Dieses kann jedoch sehr einfach durch Geldmenge und Zinsen beeinflusst werden. Außerdem kann der Wert per Knopfdruck in andere Regionen der Erde transferiert werden. Im hier vorgestellten System würde der Wert aller generierten Zertifikate spätestens nach Ende der Laufzeit wieder in der Region landen.

Es wäre bereits ein enormer Fortschritt, wenn die Menschen das bisherige System besser verstehen würden. Was ist Geld und wie entsteht es? Mit diesem System werden alle gehandelten Güter sozusagen zur eigenen Währung, was auch eine gute Grundlage für einen echten Währungswettbewerb bieten würde.

Die Dateien sind auch hier zu finden:
https://github.com/CarlFriedrichvonMises/Value-Exchange-System
https://codeberg.org/CarlFriedrichvonMises/Value-Exchange-System

MONERO

bitcoin