



(10) **DE 10 2021 212 598 A1** 2023.05.11

(12) **Offenlegungsschrift**

(21) Aktenzeichen: **10 2021 212 598.0**

(51) Int Cl.: **H04L 9/28 (2006.01)**

(22) Anmeldetag: **09.11.2021**

(43) Offenlegungstag: **11.05.2023**

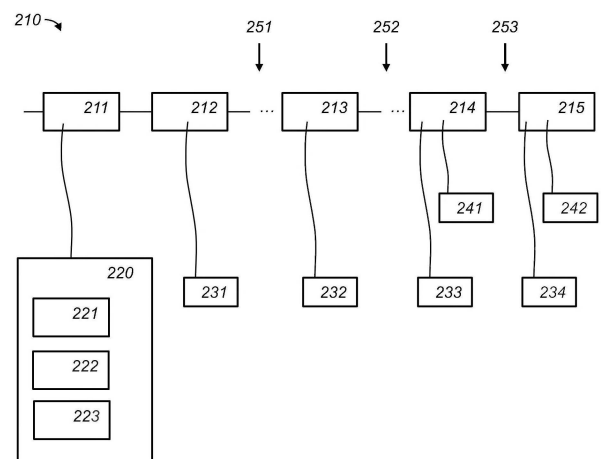
(71) Anmelder:
**Robert Bosch Gesellschaft mit beschränkter
Haftung, 70469 Stuttgart, DE**

(72) Erfinder:
Poddey, Alexander, 75446 Wiernsheim, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen.

(54) Bezeichnung: **Schutz gegen Frontrunning-Angriffe in kryptografischem Token-System**

(57) Zusammenfassung: Einige Ausführungsformen sind auf ein computer-implementiertes Verfahren zum Unterhalten von Krypto-Token eines ersten Typs gerichtet. Es werden eine Erzeugungs- und eine Vernichtungsprozedur implementiert, die eine Bindungskurve und einen Gebührenterm, beginnend von der aktuellen Angebotsgröße bis zu einer neuen Angebotsgröße, integrieren kann, um eine Menge von Krypto-Token eines zweiten Typs zu bestimmen. Die Krypto-Token des zweiten Typs können zu oder von einem Pool übertragen werden, während Krypto-Token des ersten Typs zu einem Benutzer übertragen werden können oder zerstört werden können. Der Gebührenterm kann die um eine Menge verschobene Bindungskurve umfassen.



Beschreibung

Technisches Gebiet

[0001] Der vorliegend offenbarte Gegenstand betrifft ein computer-implementiertes Verfahren zum Unterhalten von Krypto-Token eines ersten Typs, eine Server-Vorrichtung, eine Client-Vorrichtung und ein computerlesbares Medium.

Hintergrund

[0002] Ein dezentralisiertes Transaktionssystem, eine Transaktionsdatenbank oder ein verteiltes Register ist irgendein Protokoll in Computernetzen, das einen Konsens hinsichtlich seiner Transaktionen und ihrer Folge herbeiführt. Eine übliche Form eines derartigen Systems beruht auf einer Blockchain und bildet die Grundlage vieler sogenannter Kryptowährungen. In einer Kryptowährung werden kryptografische Token über mehrere Clients verteilt. Die Clients können die Token untereinander oder zu und von einem Market Maker übertragen. Kryptografie und verteilte Registersysteme stellen sicher, dass eine Übertragung nicht leicht gefälscht oder zurückgewiesen werden kann.

[0003] Das Vorliegen eines sicheren Übertragungssystems ermöglicht, dass Token eines ersten Typs gegen Token eines zweiten Typs getauscht werden. Umgangssprachlich wird ein Token des ersten Typs gekauft und weist er einen Preis als eine Menge von Token des zweiten Typs auf. Fortgeschrittene Kryptowährungen verwenden einen als „gekrümmte Bindung“ [engl.: „Curved Bonding“] genannten Mechanismus, demgemäß algorithmisch eine als eine Bindungskurve bekannte Funktion definiert wird, die den Preis von Einheiten (Token) der Währung in Abhängigkeit von dem aktuellen Angebot an Token beeinflusst.

[0004] Ein bekanntes Verfahren zum Managen einer Kryptowährung mit „gekrümmter Bindung“ ist in der internationalen Patentanmeldung WO 2019/043668 A1 offenbart. In dem bekannten Verfahren wird für eine Mehrzahl von Benutzern ein Wallet im Markt bereitgestellt, das geeignet ist, verknüpfte digitale Token zu speichern, deren Wert mit Kryptowährungs-Token verknüpft ist und die für eine Transaktion in einer digitalen Marktplattform erforderlich sind. Es wird eine Kryptowährungsreserve bereitgestellt, die geeignet ist, eine Mehrzahl von Kryptowährungs-Token zu speichern. In Ansprechen darauf, dass ein Benutzer verknüpfte digitale Token von einem Marktgeschäft kauft, werden verknüpfte digitale Token zu dem Wallet des Benutzers im Markt übertragen und wird ein äquivalenter Wert von Kryptowährungs-Token an die Kryptowährungsreserve übertragen. In Ansprechen darauf, dass ein Benutzer eine Anzahl verknüpfter digitaler Token von dem Wallet des Benutzers im Markt abhebt, werden die gewünschte Anzahl verknüpfter digitaler Token aus dem Wallet des Benutzers im Markt entnommen und wird ein äquivalenter Wert von Kryptowährungs-Token aus der Kryptowährungsreserve an ein Wallet des Benutzers außerhalb des Markts übertragen, wobei das Wallet außerhalb des Markts geeignet ist, Kryptowährungs-Token außerhalb der Marktplattform zu speichern.

[0005] Fig. 10 der erwähnten Patentanmeldung zeigt einen Graphen, der darstellt, wie die Bindung von Token angewendet werden kann. Die Token-Bindung wird verwendet, um eine Hierarchie von Token einzuführen, die grundlegend miteinander zusammenhängen. Die Token-Bindung ist ein Mittel der Token-Erzeugung mit einer vordefinierten Preis-Angebots-Beziehung oder Preis-Angebots-Kurve. Diese kann durch einen Smart Contract erzielt werden: Benutzer hinterlegen an der Adresse des Smart Contract eine Reservewährung und empfangen wiederum neu geschürfte Token. Die Einlage kann gesperrt werden, damit sie zu einem späteren Datum an Verkäufer des Tokens zurückgegeben wird. Der Preis, den der Benutzer pro Token zahlt, kann durch die oben erwähnte Kurve vorgeschrieben werden. Benutzer können zu irgendeinem Zeitpunkt in der Lage sein, ihre geschürften Token für die ursprüngliche Reservewährung zu einem durch dieselbe Kurve vorgeschriebenen Preis zu tauschen. Die Verkaufs- und die Kaufkurve können verschieden sein.

[0006] Für zusätzliche x Token, die gekauft werden sollen, kann der Smart Contract den geeigneten Punkt auf der Kurve auf der Grundlage eines vorhandenen zirkulierenden Angebots nachschlagen und die Menge bestimmen, die in dem nativen Token für das Bündel zu erzeugender x Token zu zahlen ist. Ein ähnlicher Prozess kann für das Verkaufen von Token vorgesehen sein, was diese Token dadurch, dass sie aus der Zirkulation entnommen werden, zerstört und das Gesamt-Token-Angebot entlang der Bindungskurve nach hinten bewegt. Da das Token zu 100 % abgesichert werden kann, kann das System genügend gespeicherte Reservewährung bereitstellen, um die verkauften Token zu kompensieren. Die Bindungskurve ist in dem bekannten System als

$$f(x) = \frac{x}{c(a+x^b)} \text{ mit } a > 0 \text{ und } 0,5 < b < 1; c > 1$$

definiert.

Kurzfassung

[0007] Das bekannte System ist anfällig für Frontrunning-Angriffe. Ein Frontrunning-Angriff nutzt die technischen Eigenschaften des Systems für seine eigenen Zwecke.

[0008] Durch Frontrunning einer Kauf- oder Verkaufstransaktion könnten Miner und andere Akteure Wert von normalen Teilnehmern extrahieren. Es können zwei Klassen des Frontrunning unterschieden werden: Einerseits gibt es das kurzzeitige bis mittelfristige oder hochfrequente Frontrunning (hffr) - wobei die normalen Transaktionen nicht wesentlich verzögert werden, aber eine Angriffstransaktion in der Ausführungswarteschlange vor und direkt nach der normalen Transaktion bzw. den normalen Transaktionen platziert wird. Zum Beispiel könnte ein Miner im geheimen Einverständnis stehen und eine Transaktion am vorderen Ende der Warteschlange platzieren. Zum Beispiel kann ein Benutzer mit Kenntnis einer bevorstehenden großen Transaktion seiner Frontrunning-Transaktion eine hohe Transaktionsgebühr zuordnen, um den Miner dazu zu bringen, seine Transaktion zu priorisieren. Ein Miner ist eine elektronische Vorrichtung, üblicherweise in Form einer Server-Vorrichtung, die als ein Miner konfiguriert ist.

[0009] Dass ein Teil der Miner im geheimen Einverständnis stehen, kann bestimmte Transaktionen für eine längere Zeitdauer verzögern, was als aktive Zensur bezeichnet wird. Der entsprechende Angriff wird als zensurbasiertes Frontrunning (cfr) bezeichnet. Ein Beispiel wäre das Platzieren einer Kauftransaktion, daraufhin das Sperren aller Verkaufstransaktionen und nur das Zulassen von Kauftransaktionen, schließlich das Verkaufen und somit das Extrahieren des Werts vor der Verarbeitung der verzögerten Verkaufstransaktionen.

[0010] Frontrunning-Angriffe liegen in einer ähnlichen Kategorie wie kryptografische Angriffe, Denial of Service und dergleichen. Die technischen Eigenschaften des Systems werden ausgenutzt, um den Zwecken des Angreifers zu dienen. Obwohl nichttechnische Lösungen, z. B. das Verfügen einer Rechtsprechung, die das Frontrunning verbietet, denkbar wären, ist eine technische Lösung für das Problem bevorzugt. Der Erfinder hat erkannt, dass tatsächlich technische Maßnahmen möglich sind, um diese Arten von Angriffen zu mildern.

[0011] Frontrunning-Angriffe können durch die Einführung einer Kauf/Verkaufs-Marge gemildert werden. Falls das Vernichten von Token weniger Token zurückgibt, als das Erzeugen dieser Token kostet, wird der -Angriff weniger effizient. Allerdings ist eine Bindungskurve häufig nichtlinear, so dass die gewünschte Menge der Marge keine Konstante oder konstanter Teil des Erzeugungs/Vernichtungs-Volumens ist. Die Erfinder haben ermittelt, dass dies dadurch vermieden werden kann, dass die Marge z. B. in die Form einer Gebühr gebracht wird, die anfällt, wenn die Erzeugung oder Vernichtung kryptografischer Token angefordert wird. Allerdings hat der Erfinder ermittelt, dass dies dadurch gelöst werden kann, dass die Gebühr abhängig von der Bindungskurve selbst gemacht wird.

[0012] Gemäß einer Ausführungsform werden kryptografische Token eines ersten Typs durch einen Smart Contract unterhalten. Smart Contracts sind eine vorteilhafte Art und Weise, um in verteilten Registern, die Smart Contracts unterstützen, eine neue Kryptowährung zu erzeugen. Allerdings ist ein Smart Contract nicht notwendig. Zum Beispiel könnte ein Market Maker, der dieselben Prozeduren wie der Smart Contract implementiert, Teil der Chain-Logik, z. B. der Chain-Anwendungsschicht, sein. Selbst wenn der Smart Contract woanders implementiert ist, kann ein Benutzer die Prozeduren so aufrufen, als ob sie ein in dem Register definierter Smart Contract wären. Ausführungsformen, die einen Smart Contract verwenden, können dadurch, dass die Funktionen des Smart Contract in die Chain-Logik, z. B. die Software, die das verteilte Register ausführt, aufgenommen werden, in eine Ausführungsform ohne einen Smart Contract umgewandelt werden.

[0013] Token des ersten Typs können in Tausch gegen Token eines zweiten Typs erzeugt oder vernichtet werden. Die Token des zweiten Typs können eine anerkannte Kryptowährung, z. B. Bitcoin, Ether usw., sein. Der Smart Contract kann z. B. eine Erzeugungsprozedur zum Erzeugen von Krypto-Token des ersten Typs im Tausch gegen Krypto-Token des zweiten Typs und eine Vernichtungsprozedur zum Vernichten von Krypto-Token des ersten Typs im Tausch gegen Krypto-Token des zweiten Typs implementieren. Außerdem

kann der Smart Contract Informationen, die die Token des ersten Typs betreffen, insbesondere eine aktuelle Angebotsgröße, die eine aktuelle Anzahl von Krypto-Token des ersten Typs angibt, und eine Bindungskurve, die eine Funktion definiert, unterhalten.

[0014] Zum Beispiel kann die Menge von Krypto-Token des zweiten Typs für den Tausch durch Integrieren einer Funktion von der aktuellen Angebotsgröße bis zu einer neuen Angebotsgröße berechnet werden. Dabei ist die Funktion eine Summe der Bindungskurve und einer Anzahl weiterer Terme für die Erzeugungs- und/oder Vernichtungsprozedur, wobei die weiteren Terme einen Gebührenterm enthalten, der ein Mehrfaches der um eine Menge von Krypto-Token des ersten Typs verschobenen Bindungskurve umfasst.

[0015] Zum Beispiel kann die Integration über eine Erzeugungsfunktion erfolgen, während für die Vernichtung eine Vernichtungsfunktion verwendet werden kann, falls die Erzeugungsprozedur ausgelöst wird. Beide Funktionen können gleich der Bindungskurve zuzüglich zusätzlicher Terme sein. Die Bindungskurve ist üblicherweise der Hauptterm und stellt die Langzeitentwicklung des Tokens sicher. Es kann ein Gebührenterm eingeführt werden, der die Erzeugung teurer macht, als sie sein sollte, falls nur die Bindungskurve berücksichtigt würde, während die Vernichtung weniger Token zurückerhält, als die Bindungskurve allein nahelegen würde. Somit machen die Gebührenterme einen Erzeugungs/Vernichtungs-Zyklus unattraktiv. Allerdings ist nur eine kleine Gebühr notwendig, um dies sicherzustellen, falls die Angebotsgröße in einem Gebiet liegt, in dem die Bindungskurve im Wesentlichen flach ist, während höhere Gebühren notwendig sind, um das Front-running unattraktiv zu machen, falls die Bindungskurve steil ist.

[0016] Es ist interessant, dass dies dadurch erzielt werden kann, dass der Gebührenterm proportional zu der lokalen Zunahme der Bindungskurve gemacht wird. Zum Beispiel können die Erzeugungs- und die Vernichtungsfunktion Linearkombinationen z. B. der Bindungskurve und verschobener Versionen der Bindungskurve sein. Gemäß einer Ausführungsform gibt der Gebührenterm die Flachheit der Bindungskurve an diesem Punkt an.

[0017] Ein Aspekt der Erfindung ist eine Server-Vorrichtung zum Unterhalten von Krypto-Token eines ersten Typs. Die Server-Vorrichtung kann z. B. ein sogenannter Miner sein. Ein Aspekt der Erfindung ist eine Client-Vorrichtung. Die Client-Vorrichtung kann z. B. durch einen Benutzer verwendet werden, z. B., um Erzeugungs- oder Vernichtungsanforderungen zu initiieren.

[0018] Ein weiterer Aspekt ist ein Verfahren zum Unterhalten von Krypto-Token des ersten Typs. Eine Ausführungsform des Verfahrens kann in einem Computer als ein computer-implementiertes Verfahren oder in dedizierter Hardware oder in einer Kombination beider implementiert werden. Ausführbarer Code für eine Ausführungsform des Verfahrens kann in einem Computerprogrammprodukt gespeichert sein. Beispiele von Computerprogrammprodukten enthalten Speichervorrichtungen, optische Ablagespeichervorrichtungen, integrierte Schaltungen, Server, Online-Software usw. Vorzugsweise umfasst das Computerprogrammprodukt nichttransitorischen Programmcode, der in einem computer-lesbaren Medium gespeichert ist, um eine Ausführungsform des Verfahrens auszuführen, wenn das Programm in einem Computer ausgeführt wird.

[0019] Gemäß einer Ausführungsform umfasst das Computerprogramm Computerprogrammcode, der dafür ausgelegt ist, alle oder einen Teil der Schritte einer Ausführungsform des Verfahrens auszuführen, wenn das Computerprogramm in einem Computer ausgeführt wird. Vorzugsweise ist das Computerprogramm in einem computer-lesbaren Medium verkörpert.

[0020] Ein weiterer Aspekt des vorliegend offenbarten Gegenstands ist ein Verfahren, um das Computerprogramm zum Herunterladen verfügbar zu machen.

Figurenliste

[0021] Weitere Einzelheiten, Aspekte und Ausführungsformen werden nur beispielhaft anhand der Zeichnungen beschrieben. Elemente in den Figuren sind zur Einfachheit und Klarheit dargestellt und brauchen nicht notwendig maßstabsgerecht zu sein. In den Figuren können Elemente, die bereits beschriebenen Elementen entsprechen, dieselben Bezugszeichen tragen; es zeigen schematisch:

Fig. 1a ein Beispiel einer Ausführungsform einer Client-Vorrichtung,

Fig. 1b ein Beispiel einer Ausführungsform einer Server-Vorrichtung,

Fig. 1c ein Beispiel einer Ausführungsform eines kryptografischen Token-Systems,

Fig. 2 ein Beispiel einer Ausführungsform einer Blockchain,

Fig. 3a ein Beispiel einer Ausführungsform einer Bindungskurve,

Fig. 3b ein Beispiel einer Ausführungsform einer Bindungskurve,

Fig. 3c ein Beispiel einer Ausführungsform einer Bindungskurve,

Fig. 3d ein Beispiel einer Ausführungsform einer Bindungskurve,

Fig. 4a ein Beispiel einer Ausführungsform der Aktualisierung einer Bindungskurve,

Fig. 4b ein Beispiel einer Ausführungsform einer Bindungskurve,

Fig. 4c ein Beispiel einer Ausführungsform einer Bindungskurve,

Fig. 4d ein Beispiel einer Ausführungsform einer Bindungskurve,

Fig. 5 ein Beispiel einer Ausführungsform eines Verfahrens zum Unterhalten von Krypto-Token eines ersten Typs,

Fig. 6 ein Beispiel einer Ausführungsform eines Verfahrens zum Unterhalten von Krypto-Token eines ersten Typs,

Fig. 7a ein computer-lesbares Medium mit einem beschreibbaren Teil, der ein Computerprogramm gemäß einer Ausführungsform umfasst,

Fig. 7b eine Darstellung eines Prozessorsystems gemäß einer Ausführungsform.

Bezugszeichenliste

[0022] Die folgende Liste von Bezugszeichen und Abkürzungen entspricht den **Fig. 1a-4, Fig. 7a, Fig. 7b** und ist gegeben, um die Interpretation der Zeichnungen zu erleichtern, und ist nicht als Beschränkung der Ansprüche zu verstehen.

100	ein Krypto-Token-System
110, 110.1, 110.2	eine Client-Vorrichtung
130	ein Prozessorsystem
140	ein Ablagespeicher
150	eine Kommunikationsschnittstelle
160, 160.1, 160.2	eine Server-Vorrichtung
162	eine Datenbank
170	ein Prozessorsystem
180	ein Ablagespeicher
190	eine Kommunikationsschnittstelle
172	ein Computernetz
210	eine Blockchain
211-215	ein Block
220	ein Smart Contract
221	eine Erzeugungsprozedur
222	eine Vernichtungsprozedur
223	eine Aktualisierungsprozedur
231-234	ein Zustand
241-242	eine Krypto-Token-Übertragung
251-253	ein Zeitpunkt
301	eine Bindungskurve

311	eine Menge von Krypto-Token des ersten Typs
312	eine Menge von Krypto-Token des zweiten Typs
313	eine Menge von Krypto-Token des zweiten Typs
314	eine Menge von Krypto-Token des zweiten Typs
X1, X2	eine Menge von Krypto-Token des ersten Typs
315	aktuelles Angebot von Krypto-Token des ersten Typs
330	Zustandsinformationen
321-323	Kurvensegmentparameter
324-326	Kurvensegmentparameter
341	eine Bindungskurven-Zunahme
342	ein Punkt auf der Bindungskurve
343	ein verschobener Punkt auf der Bindungskurve
1000, 1001	ein computer-lesbares Medium
1010	ein beschreibbarer Teil
1020	ein Computerprogramm
1110	eine bzw. mehrere integrierte Schaltungen
1120	eine Verarbeitungseinheit
1122	ein Speicher
1124	eine dedizierte integrierte Schaltung
1126	ein Kommunikationselement
1130	eine Verdrahtung
1140	ein Prozessorsystem

Beschreibung von Ausführungsformen

[0023] Obwohl der vorliegend offenbarte Gegenstand eine Ausführungsform in vielen verschiedenen Formen zulässt, sind in den Zeichnungen eine oder mehrere spezifische Ausführungsformen gezeigt und werden diese hier ausführlich beschrieben, wobei die vorliegende Offenbarung selbstverständlich als beispielhaft für die Prinzipien des vorliegend offenbarten Gegenstands anzusehen ist und nicht auf die spezifischen gezeigten und beschriebenen Ausführungsformen beschränkt werden soll.

[0024] Im Folgenden sind Elemente von Ausführungsformen zum Verständnis im Betrieb beschrieben. Allerdings sind die jeweiligen Elemente offenbar zum Ausführen von Funktionen, z. B. Prozeduren, ausgelegt, die als durch sie ausgeführt beschrieben werden.

[0025] Ferner ist der vorliegend offenbarte Gegenstand nicht nur auf die Ausführungsformen beschränkt, sondern enthält er außerdem jede weitere Kombination von Merkmalen, die hier beschrieben sind oder in voneinander verschiedenen abhängigen Ansprüchen angeführt sind.

[0026] **Fig. 1a** zeigt schematisch ein Beispiel einer Ausführungsform einer Client-Vorrichtung 110. **Fig. 1b** zeigt schematisch ein Beispiel einer Ausführungsform einer Server-Vorrichtung 160.

[0027] Die Server-Vorrichtung 160 kann z. B. zum Unterhalten von Krypto-Token eines ersten Typs konfiguriert sein. Die Server-Vorrichtung 160 kann z. B. zum Empfangen einer Erzeugungsanforderung zum Erzeugen von Token des ersten Typs oder einer Vernichtungsanforderung zum Vernichten von Token des ersten Typs oder einer Aktualisierungsanforderung zum Aktualisieren einer Bindungskurve konfiguriert sein. Die Server-Vorrichtung 160 kann Daten enthalten, die die eine bzw. die mehreren Transaktionen in Reaktion darauf in einem neuen Block für die Blockchain widerspiegeln. Die Informationen können die Transaktion, die zeigt, dass ein Benutzer die Token erhalten hat oder dass die Token von dem Benutzer entfernt wurden, oder Zustandsinformationen des Vertrags, die z. B. eine neue Bindungskurven-Definition oder ein neues

aktuelles Angebot usw. enthalten, widerspiegeln. Gelegentlich wird die Server-Vorrichtung als ein Miner oder als eine Mining-Vorrichtung oder als ein Schürfer oder als eine Schürfvorrichtung bezeichnet.

[0028] Die Server-Vorrichtung 160 kann konfiguriert sein, von einem verteilten Register, z. B. von einer Blockchain, einen Smart Contract zu erhalten. Der Smart Contract kann eine Erzeugungsprozedur zum Erfüllen von Erzeugungsanforderungen, eine Vernichtungsprozedur zum Erfüllen von Vernichtungsanforderungen usw. implementieren. Der Server 160 kann konfiguriert sein, den entsprechenden Computercode in dem Smart Contract auszuführen. Anstelle eines Smart Contract können die Prozeduren in herkömmlicher Software, z. B. in sogenannter Chain-Logik, implementiert sein. Die durch die Software unterhaltenen Daten können in beiden Fällen in das verteilte Register geschrieben werden. Zum Beispiel kann eine Transaktion, die die Erzeugung oder Vernichtung eines Tokens zeigt, in das verteilte Register gegeben werden, können eine aktualisierte Angebotsgröße, eine Bindungskurve und dergleichen in das verteilte Register gegeben werden.

[0029] Die Client-Vorrichtung 110 kann z. B. konfiguriert sein, ein Wallet zu unterhalten. Zum Beispiel kann die Client-Vorrichtung 110 konfiguriert sein, an die Server-Vorrichtung 160 eine Anforderung für Token des ersten Typs oder zum Vernichten von Token des ersten Typs usw. zu senden. Die Client-Vorrichtung 110 kann ebenfalls eine Aktualisierungsanforderung zum Aktualisieren der Bindungskurve senden. Zum Beispiel kann es erforderlich sein, dass eine Aktualisierungsanforderung mit einer bestimmten Identität verknüpft ist, z. B. durch einen bestimmten privaten Schlüssel signiert ist.

[0030] Die Client-Vorrichtung 110 kann ein Prozessorsystem 130, einen Ablagespeicher 140 und eine Kommunikationsschnittstelle 150 umfassen. Die Server-Vorrichtung 160 kann ein Prozessorsystem 160, einen Ablagespeicher 180 und eine Kommunikationsschnittstelle 190 umfassen. Die Ablagespeicher 140 und 180 können ein elektronischer Ablagespeicher sein. Der Ablagespeicher kann einen lokalen Ablagespeicher, z. B. ein lokales Festplattenlaufwerk oder einen elektronischen Speicher, umfassen. Der Ablagespeicher 140 und 180 kann einen nichtlokalen Speicher, z. B. einen Cloud-Speicher, umfassen. In dem letzteren Fall kann der Ablagespeicher 140 und 180 eine Ablagespeicherschnittstelle mit dem nichtlokalen Ablagespeicher umfassen.

[0031] Die Client-Vorrichtung 110 und die Server-Vorrichtung 160 können Teil eines Krypto-Token-Systems, z. B. des Krypto-Token-Systems 100, sein. Die Client-Vorrichtung 110 und die Server-Vorrichtung 160 können intern, mit anderen Systemen, mit einem externen Ablagespeicher, mit Eingabevorrichtungen, mit Ausgabevorrichtungen und/oder mit einem oder mehreren Sensoren über ein Computernetz kommunizieren. Das Computernetz kann ein Weitbereichsnetz, ein Intranet, ein LAN, ein WLAN usw. sein. Das Computernetz kann das Internet sein. Das System umfasst eine Verbindungsschnittstelle, die dafür ausgelegt ist, nach Bedarf innerhalb des Systems oder außerhalb des Systems zu kommunizieren. Zum Beispiel kann die Verbindungsschnittstelle einen Verbinder, z. B. einen verdrahteten Verbinder, z. B. einen Ethernet-Verbinder, einen optischen Verbinder usw., oder einen drahtlosen Verbinder, z. B. eine Antenne, z. B. eine WiFi-, eine 4G- oder eine 5G-Antenne, umfassen.

[0032] Die Kommunikationsschnittstelle 150 kann dafür verwendet werden, digitale Daten, z. B. eine Anforderung zum Erzeugen oder Vernichten kryptografischer Token, zu senden oder zu empfangen. Die Kommunikationsschnittstelle 190 kann dafür verwendet werden, digitale Daten, z. B. eine Anforderung zum Erzeugen oder Vernichten kryptografischer Token, zu senden oder zu empfangen. Die Kommunikationsschnittstelle 190 kann dafür verwendet werden, mit anderen Server-Vorrichtungen, z. B. zum Verteilen eines neuen Blocks einer Blockchain, zu kommunizieren.

[0033] Die Ausführung der Vorrichtungen 110 und 160 kann in einem Prozessorsystem, z. B. in einer oder mehreren Prozessorschaltungen, z. B. Mikroprozessoren, von denen Beispiele hier gezeigt sind, implementiert werden. Das Prozessorsystem kann eine oder mehrere GPUs und/oder CPUs umfassen. Die Vorrichtungen 110 und 160 des Systems 100 können mehrere Prozessoren umfassen, die über verschiedene Orte verteilt sein können. Zum Beispiel können die Vorrichtungen 110 und 160 Cloud-Computing verwenden.

[0034] Die Vorrichtungen 110 und 160 können Funktionseinheiten umfassen, die Funktionseinheiten des Prozessorsystems sein können. Zum Beispiel können die gezeigten Funktionseinheiten vollständig oder teilweise in Computeranweisungen implementiert sein, die in der Vorrichtung, z. B. in einem elektronischen Speicher der Vorrichtung, gespeichert sind und durch einen Mikroprozessor der Vorrichtung ausführbar sind. In Hybridausführungsformen werden Funktionseinheiten teilweise in Hardware, z. B. als Coprozessoren, z. B. als kryptografische Coprozessoren, implementiert und teilweise in Software gespeichert und in der Vorrichtung ausgeführt.

[0035] Fig. 1c zeigt schematisch ein Beispiel einer Ausführungsform eines kryptografischen Token-Systems. Das System 100 umfasst mehrere Client-Vorrichtungen; es sind die Client-Vorrichtungen 110.1 und 110.2 gezeigt. Das System 100 umfasst mehrere Server-Vorrichtungen; es sind die Server-Vorrichtungen 160.1 und 160.2 gezeigt. Die Vorrichtungen sind über ein Computernetz 172, z. B. über das Internet, verbunden. Die Client- und die Server-Vorrichtung können gemäß einer Ausführungsform sein. Die Client-Vorrichtungen können miteinander zusammenwirken, um kryptografische Token des ersten Typs zu übertragen. Die Client-Vorrichtungen können mit einer Server-Vorrichtung zusammenwirken, um ein kryptografisches Token des ersten Typs, z. B. im Tausch gegen kryptografische Token des zweiten Typs, zu erzeugen oder zu vernichten.

[0036] Der Ablagespeicher kann als ein elektronischer Speicher, angenommen ein Flash-Speicher, oder als ein magnetischer Speicher, angenommen eine Festplatte oder dergleichen, implementiert sein. Der Ablagespeicher kann mehrere diskrete Speicher umfassen, die zusammen den Ablagespeicher 140, 180 ergeben. Der Ablagespeicher kann einen temporären Speicher, angenommen einen RAM, umfassen. Der Ablagespeicher kann ein Cloud-Ablagespeicher sein.

[0037] Üblicherweise umfassen die Client-Vorrichtung 110 und die Server-Vorrichtung 160 jeweils einen Mikroprozessor, der geeignete Software ausführt, die in dem System gespeichert ist; wobei diese Software z. B. heruntergeladen und/oder in einem entsprechenden Speicher, z. B. einem flüchtigen Speicher wie etwa einem RAM oder einem nichtflüchtigen Speicher wie etwa einem Flash, gespeichert worden sein kann. Alternativ können die Systeme ganz oder teilweise in programmierbarer Logik, z. B. als eine frei programmierbare logische Anordnung (FPGA), implementiert sein. Die Systeme können ganz oder teilweise als eine sogenannte anwendungsspezifische integrierte Schaltung (ASIC), z. B. als eine integrierte Schaltung (IC), die für ihre bestimmte Verwendung nutzerangepasst ist, implementiert sein. Zum Beispiel können die Schaltungen in CMOS, z. B. unter Verwendung einer Hardwarebeschreibungssprache wie etwa Verilog, VHDL usw., implementiert sein. insbesondere können die Client-Vorrichtung 110 und die Server-Vorrichtung 160 Schaltungen für die kryptografische Verarbeitung und/oder arithmetische Verarbeitung umfassen.

[0038] Eine Prozessorschaltung kann auf verteilte Weise, z. B. als mehrere Teilprozessorschaltungen, implementiert sein. Ein Ablagespeicher kann über mehrere verteilte Unterablagenspeicher verteilt sein. Ein Teil oder der gesamte Speicher kann ein elektronischer Speicher, ein magnetischer Speicher usw. sein. Zum Beispiel kann der Ablagespeicher einen flüchtigen und einen nichtflüchtigen Teil aufweisen. Ein Teil des Ablagespeichers kann nur lesbar sein.

[0039] Fig. 2 zeigt schematisch ein Beispiel einer Ausführungsform einer Blockchain 210. Blockchains sind ein bestimmtes Beispiel für verteilte Register, von denen gezeigt worden ist, dass sie gemäß Ausführungsformen gut arbeiten. Andere Beispiel für verteilte Register können ebenfalls verwendet werden. Zum Beispiel kann das verteilte Register gemäß einer Ausführungsform ein Hash-Graph, ein Tangle oder ein Gitter sein. Das verteilte Register umfasst mehrere Blöcke, die miteinander verknüpft sind. Die Blöcke können Transaktionsdaten und Metadaten umfassen. Die Metadaten können Verknüpfungsinformationen und einen Konsensmechanismus umfassen. Ausführungsformen sind hauptsächlich mit Bezug auf eine Blockchain beschrieben, wobei aber eine derartige Ausführungsform geändert werden könnte, um einen anderen Typ eines verteilten Registers, insbesondere einen Graphen-basierten, zu verwenden.

[0040] Die Blockchain 210 umfasst mehrere Blöcke, die in einer Folge miteinander verknüpft sind. Die Verknüpfung kann z. B. einen Konsensmechanismus umfassen. Ein derartiger Mechanismus kann z. B. ein Proof of Work, z. B. wie in Bitcoin, sein. Der Mechanismus kann ein Proof of Stake sein. Ein Konsensmechanismus ermöglicht ein verteiltes Vertrauen in das verteilte Register. Gemäß einer Ausführungsform kann ein anderer Konsensmechanismus, z. B., wie er im Gebiet bekannt ist, verwendet werden.

[0041] Zur Hilfe bei der Diskussion zeigt Fig. 2 drei Punkte in der Blockchain: die Punkte 251, 252 und 253, die drei Zeitpunkten entsprechen. Beim Punkt 251 sind Blöcke bis zum Block 213, aber noch nicht der Block 213, erzeugt worden. Beim Punkt 252 sind Blöcke bis zum Block 214, aber noch nicht der Block 214, erzeugt worden. Beim Punkt 253 sind Blöcke bis zum Punkt 215, aber noch nicht der Block 215, erzeugt worden.

[0042] In der Blockchain 210 sind mehrere Blöcke, in diesem Fall 5 Blöcke, gezeigt: die Blöcke 211, 212, 213, 214 und 215. Es kann mehr oder weniger Blöcke geben. Ein Block kann Daten, die sich auf den Mechanismus eines verteilten Registers beziehen, z. B. Konsensdaten, aber ebenfalls andere Informationen, umfassen. Insbesondere kann ein Block Transaktionen, in denen Token an eine Adresse gebunden sind, z. B. auf den öffentlichen Schlüssel eines Clients bezogen sind, der z. B. in einer Client-Vorrichtung enthalten ist, umfassen. Außerdem können Blöcke andere Informationen enthalten.

[0043] Insbesondere kann ein Block einen Smart Contract umfassen. Der Block 211 zeigt ein Beispiel in Form eines Smart Contract 220. Üblicherweise ist ein Smart Contract in einer Computersprache geschrieben. Ein Beispiel einer Computersprache, die für Smart Contracts optimiert ist, ist Solidity. Zum Beispiel kann die Blockchain 210 gemäß einer Ausführungsform die Ethereum-Blockchain sein und kann der Smart Contract in Solidity geschrieben sein. Allerdings ist es nicht erforderlich, auf eine bestimmte Sprache oder Blockchain zu beschränken. Zum Beispiel kann die Ethereum-Blockchain verwendet werden, wie sie in der Abhandlung „Ethereum: a secure decentralised generalised transaction ledger“ von G. Wood, z. B. die Istanbul-Version 80085f7 vom 11.07.2021, beschrieben ist.

[0044] Zum Beispiel kann gemäß einer Ausführungsform ein zum Unterhalten von Krypto-Token eines ersten Typs konfigurierter Server konfiguriert sein, den Smart Contract von dem verteilten Register zu erhalten. Der Smart Contract kann z. B. in einem Block des verteilten Registers gespeichert sein. Der Smart Contract kann die notwendigen Prozeduren, z. B. eine Erzeugungsprozedur zum Erzeugen der Krypto-Token des ersten Typs und eine Vernichtungsprozedur für die Vernichtung von Krypto-Token des ersten Typs, implementieren. Der Smart Contract kann ebenfalls eine Aktualisierungsprozedur implementieren. Der Smart Contract kann konfiguriert sein, die aktuelle Angebotsgröße zu unterhalten. Der Smart Contract kann die Bindungskurve definieren.

[0045] Gemäß einer Ausführungsform wird die Blockchain 210 zum Erzeugen und Vernichten kryptografischer Token eines ersten Typs verwendet. Umgangssprachlich wird das Erzeugen neuer kryptografischer Token gelegentlich als ‚Kaufen‘ der Token bezeichnet; das Vernichten eines kryptografischen Tokens wird gelegentlich als ‚Verkaufen‘ der Token bezeichnet.

[0046] Der Smart Contract implementiert mehrere Prozeduren, einschließlich wenigstens einer Erzeugungsprozedur 221 und einer Vernichtung 222 (auch eine Verkaufsprozedur genannt). Optional kann der Contract eine Aktualisierungsprozedur 223 implementieren. Umgangssprachlich wird die Erzeugungsprozedur ebenfalls eine Kaufprozedur und die Vernichtungsprozedur 222 eine Verkaufsprozedur genannt. Dies ist nicht ganz genau, da die Token üblicherweise nicht mehr vorhanden sind, wenn sie vernichtet worden sind. Das Gesamtangebot von Token nimmt nach einer Vernichtungsaktion ab. Die Vernichtungsprozedur wird ebenfalls als eine Zerstörungsprozedur bezeichnet.

[0047] Der Server führt die Erzeugungsprozedur aus und erhält als Ergebnis einen neuen Zustand. Der neue Zustand kann z. B. die erhöhte Anzahl von Krypto-Token eines ersten Typs, die nun vorhanden sind, (als das Angebot bezeichnet) widerspiegeln. Außerdem kann der Server eine Transaktion, die angibt, dass die neuen kryptografischen Token an den ersten Benutzer übertragen werden, und/oder eine Transaktion, die angibt, dass die vorhandenen kryptografischen Token des zweiten Typs von dem ersten Benutzer an ein dem Smart Contract zugeordnetes Wallet übertragen werden, erhalten. Der Smart Contract wird als der Market Maker bezeichnet. Eine Menge von Token des zweiten Typs kann durch den Market Maker, z. B. im Wallet, in Reserve gehalten werden. Dieser Teil des Wallets wird als der Pool oder Pool-Saldo bezeichnet. Dasselbe Wallet kann verwendet werden, um Token zu halten, die nicht Teil des Pools sind. Die Verwendung dieses Wallets kann auch nur für den Pool reserviert werden.

[0048] Der Server-Client schreibt in die Blockchain, enthält z. B. in einem Block den neuen Zustand und die neuen Krypto-Token des ersten Typs, wobei die übertragenen Krypto-Token des zweiten Typs in diese oder in eine andere Blockchain geschrieben werden. Token des ersten Typs und des Zustands können ebenfalls in getrennte Blockchains gelegt werden.

[0049] Es wird angenommen, dass ein erster Benutzer eine Anzahl von Krypto-Token eines ersten Typs kaufen möchte. Er sendet über eine Client-Vorrichtung eine Anforderung an eine Server-Vorrichtung. Die Anforderung kann an mehrere Server-Vorrichtungen gesendet werden. Die Anforderung kann z. B. Folgendes enthalten:

- die Menge x angeforderter Krypto-Token eines ersten Typs
- Anweisungen zum Übertragen von y Krypto-Token eines zweiten Typs
- eine Adresse, um die Krypto-Token eines ersten Typs an sie zu binden.

[0050] Zum Beispiel wird betrachtet, dass die Anforderung am Punkt 252, unmittelbar, bevor der Block 214 erzeugt wird, gesendet wird.

[0051] Die Server-Vorrichtung liest den Smart Contract 220 aus der Blockchain aus. Der Smart Contract verwendet einen Zustand, der aktualisiert werden kann. Die Server-Vorrichtung liest den aktuellen Zustand aus der Blockchain aus. Die Blockchain 210 zeigt die Zustände 231 und 232 vor dem Punkt 252, so dass die Server-Vorrichtung den Zustand 232 ausliest.

[0052] Um die Menge kryptografischer Token des zweiten Typs (y) zu bestimmen, die gegen eine Menge kryptografischer Token des ersten Typs (x) getauscht werden, umgangssprachlich als der Preis bezeichnet, verwendet der Smart Contract eine Bindungskurve. Der Smart Contract kann eine Definition der Bindungskurve umfassen. Die Definition der Bindungskurve kann ebenfalls in einem Zustand sein. Die Definition der Bindungskurve kann der Smart Contract sein, bis sie eine neue Definition in einem geschriebenen Zustand überschreibt. Es wird angemerkt, dass eine Bindungskurve üblicherweise wachsend oder wenigstens nicht fallend ist.

[0053] Gemäß einer Ausführungsform ist der Smart Contract nicht in einem Block gespeichert, sondern für den Server über andere Mittel zugreifbar; z. B. kann der Smart Contract vor dem Ausführen der Prozeduren erhalten werden. Die Verwendung eines Smart Contract kann den Vorteil haben, dass ein Beweis für die Ausführung, z. B. irgendeiner bestimmten Prozedur, in dem verteilten Register angeordnet werden kann. Es wird angemerkt, dass selbst dann, wenn in der Chain kein Smart Contract angeordnet ist, er immer noch als einer ausgeführt werden kann, sofern andere Miner Zugriff auf seinen Code haben.

[0054] Tatsächlich brauchen die Prozeduren nicht einmal in einem Smart Contract implementiert zu sein, sondern können sie in herkömmlicher Software implementiert sein. Zum Beispiel kann derartige Software durch den Server vor der Ausführung erhalten werden. Die Software kann Teil der Chain-Logik-Software sein, die die Mining-Operation definiert hat.

[0055] Gemäß einer Ausführungsform könnte der Market Maker, z. B. der Smart Contract oder andere Software, Teil der Chain-Anwendungsschicht sein. Ein Benutzer kann die Prozeduren wie in einem Smart Contract aufrufen.

[0056] Falls kein Smart Contract verwendet wird, kann das Wallet oder der Pool, das bzw. der dem Smart Contract zugeordnet ist, durch ein Wallet oder einen Pool, das bzw. der dem Market Maker zugeordnet ist, z. B. durch die Software, die die Kryptowährung implementiert, ersetzt werden.

[0057] Fig. 3a zeigt schematisch ein Beispiel einer Ausführungsform einer Bindungskurve 301. Auf der x-Achse 311 ist die Menge der Krypto-Token des ersten Typs. Auf der y-Achse 312 ist die Menge der Krypto-Token des zweiten Typs.

[0058] Es wird angenommen, dass das Angebot von Token des ersten Typs aktuell X_1 ist und dass der Benutzer ($X_2 - X_1$) Token erhalten möchte, so dass das neue Angebot X_2 wird. Um die Menge von Token des zweiten Typs zu bestimmen, die getauscht werden sollen, wird eine Funktion von X_1 bis X_2 integriert. Im Fall der Erzeugung von Token kann diese Funktion als die Erzeugungsfunktion bezeichnet werden. Üblicherweise ist eine Bindungskurve wachsend oder wenigstens nicht fallend.

[0059] Gleichfalls wird angenommen, dass das Angebot von Token des ersten Typs aktuell X_2 ist und dass der Benutzer ($X_2 - X_1$) Token des ersten Typs vernichten möchte, so dass das neue Angebot X_1 wird. Um die Menge an Token des zweiten Typs zu bestimmen, die empfangen werden sollen, wird eine Funktion von X_1 bis X_2 integriert. Im Fall des Vernichtens von Token kann diese Funktion als die Vernichtungsfunktion bezeichnet werden.

[0060] Gemäß einer Ausführungsform kann die Funktion, die integriert wird, z. B. die Erzeugungsfunktion oder die Vernichtungsfunktion, als eine Summe von Termen dargestellt werden. Der erste Term kann die Bindungskurve sein. Üblicherweise ist der Bindungskurven-Term der Hauptterm, z. B. größer als die anderen Terme.

[0061] In bekannten Systemen kann die Funktion nur die Bindungskurve sein, wobei dies in dem Sinn wirken würde, dass Token des ersten oder des zweiten Typs zuverlässig gegen Token des zweiten oder des ersten Typs getauscht werden können, wobei diese Systeme aber anfällig für einen als Frontrunning bekannten Angriff sind. Falls ein Angreifer die Reihenfolge, in der Bestellungen verarbeitet werden, oder die Reihenfolge, in der seine Bestellung relativ zu anderen Bestellungen verarbeitet wird, beeinflussen kann, kann er künstlich sicherstellen, dass die Bestellung eine Vorzugsbehandlung empfängt. Diese sind als Frontrunning-

Angriffe bekannt. Um dieses Risiko zu mildern, kann die Funktion, die integriert wird, zusätzlich zu der Bindungskurve einen Gebührenterm enthalten. Der Gebührenterm macht das Frontrunning weniger vorteilhaft oder sogar unvorteilhaft.

[0062] Gemäß einer Ausführungsform umfasst der Gebührenterm ein Mehrfaches der Bindungskurve, verschoben um eine Menge von Krypto-Token des ersten Typs, z. B. s_{fr} . Zum Beispiel kann die verschobene Bindungskurve $\Gamma(x + s_{fr})$ oder $\Gamma(x - s_{fr})$ sein, falls die Bindungskurve $\Gamma(x)$ ist. Der Gebührenterm kann auch die Bindungskurve umfassen ist $\Gamma(x)$ selbst. Zum Beispiel können die Gebührenterme eine Differenz derartiger Terme oder ein Vielfaches davon sein. Das heißt, der Gebührenterm kann von der Form $\gamma(\Gamma(x + s_{fr}) - \Gamma(x))$ sein, worin γ eine Zahl, z. B. eine reelle Zahl, z. B. eine Zahl zwischen 0 und 1, z. B. 0,5 oder dergleichen, ist. Die Differenz $dl = \Gamma(x + s_{fr}) - \Gamma(x)$ kann ebenfalls auf andere Weise, z. B. mit einem Exponenten, dl^γ , oder in einem Polynom, $P(dl)$, usw. gewichtet werden. Der Differenzterm dl repräsentiert die Flachheit der Bindungskurve um x .

[0063] Ein Vorteil, dass ein Term wie $\gamma(\Gamma(x + s_{fr}) - \Gamma(x))$ in einem Gebührenterm enthalten ist, ist, dass der Gebührenterm klein ist, falls die Angebotsgröße groß ist. Das heißt, falls das System reif ist und die Bindungskurve recht flach ist, können mit Frontrunning nur kleine Gewinne gemacht werden, falls das System aber noch nicht reif ist und die Bindungskurve steil ist, ist die Gebühr hoch und ist das Frontrunning dementsprechend weniger vorteilhaft.

[0064] Fig. 3a zeigt die Bindungskurve und die Integration, wobei die Integration gemäß einer Ausführungsform ebenfalls über einen Gebührenterm erfolgt. Zusätzlich zu der Integration kann zu der Menge von Token des zweiten Typs, die übertragen oder empfangen werden, ein konstanter Term addiert oder davon subtrahiert werden. Über den konstanten Term wird üblicherweise nicht integriert, obwohl es möglich wäre.

[0065] Es wird angemerkt, dass $X1$ und $X2$ ganze Zahlen sein können, wobei dies aber nicht notwendig ist. Token können ebenfalls in Bruchteilen ganzzahliger Token erzeugt und vernichtet werden. Ein neuer Zustand, der in das Register geschrieben wird, kann enthalten, dass das neue Angebot von Token $X2$ ist.

[0066] Zum Beispiel können Token des ersten Typs ein neuer Typ von Token sein, die gemäß einer Ausführungsform erzeugt werden, z. B., um einige neue Anwendungen zu ermöglichen, die ein Token-Management erfordern. Dies könnte von Geschäften bis zu Spielen, zu Diensten, zu Partnervermittlungsanwendungen reichen. Token des zweiten Typs sind üblicherweise vorhandene Token, die digital übertragen werden können. Die Token des zweiten Typs können z. B. Bitcoin oder Ether oder dergleichen sein.

[0067] Üblicherweise wird die Bindungskurve nur verwendet, wenn Token in Bezug auf den Market Maker erzeugt oder vernichtet werden. Die Token des ersten Typs könnten ebenfalls auf einem Sekundärmarkt übertragen werden und in der Theorie können die Token gegen alles getauscht werden, was die Beteiligten vereinbaren. Da beide Beteiligte ebenfalls die Option haben, Token von dem Market Maker zu erhalten oder sie von dem Market Maker vernichten zu lassen, hat die Bindungskurve allerdings einen starken Einfluss auf den Sekundärmarkt. Eine Motivation für die Verwendung von Bindungskurven ist, große Preisschwankungen zu vermeiden.

[0068] Die Bindungskurve kann eine S-Form oder Sigmoidform aufweisen, wie sie z. B. in Fig. 3a gezeigt ist. Wenn das Angebot auf der x-Achse klein ist, können die Token leicht erhalten werden. Wenn der Markt reif ist, konvergiert der Preis üblicherweise auf einen Wert 314. Allerdings ist dies nicht notwendig. Anstelle einer Konvergenz kann der Preisanstieg z. B. viel flacher als in dem Mittelteil von Fig. 3a sein. Allerdings ist eine Sigmoidform nicht notwendig. Zum Beispiel kann eine Bindungskurve eine nach oben gebogene Form aufweisen.

[0069] Gemäß einer Ausführungsform ist die Bindungskurve durch mehrere Kurvensegmente definiert. Die mehreren Segmente sind verkettet und definieren zusammen die Bindungskurve. Dies hat den Vorteil, dass für die verschiedenen Kurvensegmente verschiedene Gleichungen verwendet werden können. Falls zum Definieren der gesamten Kurve eine Funktion verwendet würde, wäre dies eine komplizierte Funktion, um sie an die gewünschte Form der Kurve anzupassen. Eine derartige komplizierte Funktion ist schwer zu integrieren.

[0070] Andererseits würde entlang des Segments oder der Segmente, die diesen Teil der Bindungskurve definieren, integriert, wenn Segmente verwendet werden.

[0071] Die Form eines Kurvensegments kann durch Parameter definiert werden. Zum Beispiel kann sie durch Koeffizienten definiert werden. Zum Beispiel kann ein Kurvensegment eine Polynomkurve sein. Zum Beispiel können sie Polynome eines niedrigen Grads, z. B. höchstens 5. Grads, höchstens 4. Grads, höchstens 3. Grads, sein. In Experimenten wurde ermittelt, dass die Verwendung von drei Kurvensegmenten und Polynomen 3. Grads (kubischen Polynomen) gut funktioniert hat; allerdings kann eine Bindungskurve ebenfalls mit weniger, z. B. 1 oder 2, oder mehr Kurvensegmenten definiert werden.

[0072] Gemäß einer Ausführungsform verwenden die Erzeugungsprozedur und die Vernichtungsprozedur dieselbe Bindungskurve.

[0073] Dementsprechend kann die Erzeugungsprozedur 221 in dem Smart Contract 220 konfiguriert sein zum:

- Integrieren der Erzeugungsfunktion von dem aktuellen Angebot bis zu dem aktuellen Angebot + x, um die geforderte Menge von Krypto-Token des zweiten Typs zu erhalten,
- Übertragen der Krypto-Token des zweiten Typs an einen dem Smart Contract zugeordneten Pool,
- Erhöhen des aktuellen Angebots um x und Binden von x Krypto-Token des ersten Typs an die Adresse.

[0074] Dementsprechend kann der Block 214 einen neuen Zustand 233 umfassen, z. B. das neue Angebot und eine bzw. mehrere Transaktionen 241 umfassen.

[0075] Eine Vernichtungsprozedur kann umgekehrt funktionieren. Zum Beispiel kann eine Anforderung zum Vernichten von x Krypto-Token des ersten Typs durch die Vernichtungsprozedur 222 wie folgt implementiert werden:

- Integrieren der Vernichtungsfunktion von dem aktuellen Angebot -x bis zu dem aktuellen Angebot, um die geforderte Menge von Krypto-Token des zweiten Typs zu erhalten,
- Übertragen der Krypto-Token des zweiten Typs von dem dem Smart Contract zugeordneten Pool zu einer dem Benutzer zugeordneten Adresse,
- Kennzeichnen der x Krypto-Token des ersten Typs als ungültig für den Benutzer,
- Verringern des aktuellen Angebots um x.

[0076] Falls die Vernichtungsanforderung z. B. am Punkt 253 empfangen wird, kann der Block 215 einen neuen Zustand 234 umfassen, z. B. das neue Angebot und eine bzw. mehrere Transaktionen 242 umfassen.

[0077] Falls kein Smart Contract verwendet wird, kann der Pool dem Market Maker zugeordnet sein.

[0078] Das Ergebnis der Erzeugungs- oder Vernichtungsprozedur können eine oder zwei Transaktionen der Token des ersten bzw. des zweiten Typs und ein neuer Zustand sein. Diese drei Positionen können in eine Blockchain wie etwa in die Blockchain 210 geschrieben werden.

[0079] Sowohl die Erzeugungs- als auch die Vernichtungsprozedur kann das Ausführen der Erzeugungs- oder Vernichtungsaufgabe ablehnen, falls Vorbedingungen nicht erfüllt sind. Zum Beispiel sollte die Menge an Krypto-Token des zweiten Typs, die für eine Erzeugungsanforderung verfügbar sind, groß genug, z. B. wenigstens so groß, wie das Integral angibt, sein. Zum Beispiel sollte die Menge an Krypto-Token des zweiten Typs, die in dem Pool für eine Vernichtungsanforderung verfügbar sind, groß genug, z. B. wenigstens so groß, wie das Integral angibt, sein. Die zweite Bedingung kann dadurch erzwungen werden, dass erzwungen wird, dass die Größe des Pools immer gleich der Größe des Integrals der Vernichtungsfunktion von 0 bis zu dem aktuellen Angebotspunkt ist.

[0080] Die Aktualisierungsprozedur 223 kann aufgerufen werden, um die Form der Bindungskurve zu ändern. Beispiele der Aktualisierungsprozedur 223 sind hier gegeben.

[0081] Zur Vollständigkeit zeigt **Fig. 3b** schematisch ein Beispiel einer Ausführungsform einer Bindungskurve, wie sie verwendet werden kann, wenn der Markt am Anfang steht. Es sind drei Phasen, gelegentlich Regimes genannt, gezeigt. In einem ersten Regime I werden Token des ersten Typs erzeugt. Obwohl die Bindungskurve angibt, dass Token des zweiten Typs gegen sie getauscht werden sollten, um einen Pool zu füllen, erfolgt dies im Regime I nicht. Zum Beispiel können diese Token als ein Anreiz für frühe Investoren, Erfin-

der und dergleichen verwendet werden. In einer zweiten Phase oder im Regime II werden Token des ersten Typs gegen Token des zweiten Typs getauscht. Allerdings wird anstelle des durch die Bindungskurve angegebenen Preises ein konstanter Preis 313 verwendet. Der Preis wird in der Weise gewählt, dass die Größe des Pools (in Token des zweiten Typs) an dem Ende des Regimes II so groß wie das Integral der Bindungskurve bis zu dem Ende des Regimes II ist. Das Regime II kann z. B. verwendet werden, um das System zu starten. Diese Aufgaben können z. B. frühe Investoren ausführen. Im Regime III folgen die Preise der wie oben angegebenen Bindungskurve. Falls das Angebot vom Regime III in den Teil der Kurve für das Regime II oder I fällt, werden die normalen Preise verwendet, wie sie durch die Bindungskurve angegeben sind. Es sind verschiedene Verfeinerungen möglich. Zum Beispiel kann das System das Vernichten von Token ablehnen, falls das veranlassen würde, dass das Angebot zwischen einer bestimmten Menge fällt. Es können zwei Bindungskurven verwendet werden usw.

[0082] Gemäß einer Ausführungsform unterhält der Market Maker z. B. in einem Zustand in dem verteilten Register ein aktuelles Angebot von Token des ersten Typs. Zum Beispiel zeigt **Fig. 3b** bei 315 das aktuelle Angebot von Token. Falls Token des ersten Typs erzeugt werden, wird die Menge von Token des zweiten Typs, die dafür notwendig sind, durch Integrieren der Kurve, beginnend vom Punkt 315 nach rechts; d. h. in Richtung eines höheren Angebots, während Token erzeugt werden, erhalten. Falls Token des ersten Typs vernichtet werden, wird die Menge von Token des zweiten Typs, die dafür angeboten werden, durch Integrieren der Kurve, beginnend vom Punkt 315 nach links; d. h. in Richtung eines niedrigeren Angebots, während Token zerstört werden, erhalten.

[0083] Eine Bindungskurve kann durch Parameter definiert werden. Dies hat Vorteile, da es die Menge an Daten verringert, die in dem Register, z. B. in dem Smart Contract oder bei einer Aktualisierung der Bindungskurve, gespeichert werden müssen. Eine Bindungskurve kann ebenfalls außerhalb der Chain, z. B. in der Chain-Logik, definiert werden. Vorzugsweise kann das Integral der Bindungskurve hinsichtlich der Parameter, z. B. als eine Funktion, die die Parameter als Eingabe nimmt, ausgedrückt werden. Dies verringert die Menge der Berechnung in der Chain. Eine Bindungskurve kann z. B. als ein oder mehrere Splines, Geraden, Polynome, Polynomsegmente definiert werden.

[0084] **Fig. 3c** zeigt schematisch ein Beispiel einer Ausführungsform einer Bindungskurve. In **Fig. 3c** sind drei Kurvensegmente: die Segmente A, B und C, gezeigt. Die Verwendung der Kurvensegmente ist eine zweckmäßige Art und Weise, eine Bindungskurve in einem Smart Contract und dergleichen zu codieren.

[0085] Die Bindungskurve ist in jedem Kurvensegment durch einen oder mehrere Parameter definiert. Zum Beispiel definieren die Parameter 321 das Segment A, definieren die Parameter 322 das Segment B und definieren die Parameter 323 das Segment C. insbesondere, falls die Bindungskurve aktualisierungsfähig ist, können die Parameter 321-323 in dem Zustand enthalten sein. Außerdem ist in der **Fig. 3c** das Angebot 330, d. h. die Menge an Token des ersten Typs, die aktuell vorhanden sind, z. B. die Summe erfolgreicher Erzeugungsanforderungen minus der Summe erfolgreicher Vernichtungsanforderungen, gezeigt.

[0086] Eine zweckmäßige Art und Weise, die Kurvensegmente zu definieren, ist die Verwendung von Polynomen. Die Parameter 321-323 können die Koeffizienten der Polynome umfassen. Die Exponenten in Polynomen sind ganzzahlig. Die Kurven können durch sogenannte verallgemeinerte Polynome, z. B. Summen der Terme in der Form ax^b , wobei b eine nicht ganze Zahl, üblicherweise aber rational, sein kann, definiert werden. Verallgemeinerte Polynome haben mit regulären Polynomen gemeinsam, dass sie leicht und in geschlossener Form integriert werden können. Polynome können zweckmäßig in Form von Bázier-Splines ausgedrückt werden.

[0087] Es ist möglich, dass die Segmente, z. B. die Segmente A, B und C, derselben Unterteilung wie die Regimes I, II und III, folgen, wobei dies aber nicht notwendig ist. Im Gegenteil wurde ermittelt, dass eine Flexibilität bei der Wahl, wo Segmente beginnen und enden, eine bessere Anpassung ermöglichen kann. Zum Beispiel kann das Segment A größer als das Regime I sein, während das Segment B kleiner als das Regime II sein kann. Das Regime III kann vor dem Segment C beginnen. Wo sich die besten Punkte für den Beginn und das Ende von Segmenten befinden, kann von der Anpassung der Kurven abhängen.

[0088] Ein Gebührenterm kann ebenfalls als eine Funktion ausgedrückt werden, die ähnlich, z. B. unter Verwendung eines oder mehrerer durch Parameter, z. B. Polynomparameter, definierter Kurvensegmente, definiert werden kann. Ein Vorteil, den Gebührenterm hinsichtlich der Bindungskurve, z. B. als eine Linearkombination einer oder mehrerer Verschiebungen der Bindungskurve, auszudrücken, ist, dass, möglicherweise mit Ausnahme des Betrags der Verschiebung, kein neuer Satz von Parametern notwendig ist. Die Verschiebung

kann vorgegeben, z. B. fest codiert, z. B. Teil der Chain-Logik, sein. Die Verschiebung kann konfigurierbar, z. B. Teil eines in der Blockchain gesicherten Zustands, sein. Diese Verschiebung kann dynamisch, z. B. aus früheren Transaktionen, z. B. aus früheren Transaktionen, wie sie in dem Register sichtbar sind, bestimmt werden.

[0089] Fig. 3d zeigt schematisch ein Beispiel einer Ausführungsform einer Bindungskurve. Gezeigt sind eine aktuelle Menge x und die verschobene Menge $x + s_{fr}$. Der Wert der Bindungskurve bei x ist mit 342 angegeben, z. B. $\Gamma(x)$, und der Wert der Bindungskurve des verschobenen Orts ist bei 343 angegeben, z. B. $\Gamma(x + s_{fr})$. Die Differenz ist bei 341 angegeben, z. B. $\Gamma(x + s_{fr}) - \Gamma(x)$. Der Gebührenterm kann ein Mehrfaches der Differenz umfassen.

[0090] Gemäß einer Ausführungsform wird eine Funktion von einer aktuellen Angebotsgröße bis zu einer neuen Angebotsgröße integriert, um die Menge der Krypto-Token des zweiten Typs für den Tausch zu bestimmen. Zum Beispiel kann diese für die Erzeugung einer Erzeugungsfunktion sein; kann diese für die Vernichtung eine Vernichtungsfunktion sein. Die Funktion kann eine Summe der Bindungskurve und einer Gebühr sein. Der Betrag kann die Summe der Integration und Transaktionskosten sein. Üblicherweise sind die Transaktionskosten für die Erzeugung positiv und für die Vernichtung negativ. Die Integration kann durch einen Smart Contract erfolgen.

[0091] Die Erzeugungsfunktion kann z. B. die Summe der Bindungskurve und eines Gebührenterms $\Gamma(x) + \sigma_{p,b}$ sein; die Vernichtungsfunktion kann der Rest der Bindungskurve minus einem Gebührenterm $(\Gamma(x) - \sigma_{p,s})$ sein. Üblicherweise werden die Gebührenterme in der Weise gewählt, dass die resultierende Erzeugungs- oder Vernichtungsfunktion positiv bleibt. Jede Funktion kann über das Intervall zwischen dem aktuellen Angebot und dem neuen Angebot integriert werden. Die Richtung der Integration kann in der Weise gewählt werden, dass der Betrag positiv ist.

[0092] Der Gebührenterm kann ein Mehrfaches der Bindungskurve, verschoben um eine Menge von Krypto-Token des ersten Typs s_{fr} umfassen. Die Menge der Krypto-Token s_{fr} kann in der Weise gewählt werden, dass die Menge des Handels, von dem erwartet wird, dass ein Angreifer in der Lage ist, ihn zu beeinflussen, kleiner ist. Wird z. B. angenommen, dass alle wenigen Stunden neue Blöcke zu dem Register hinzugefügt werden, kann die Menge der Token für die Verschiebung s_{fr} als die erwartete Anzahl von Krypto-Token des ersten Typs, die an Erzeugungs- und/oder Vernichtungsaktionen beteiligt sind, gewählt werden.

[0093] Der Gebührenterm kann proportional zu der Zunahme der Bindungskurve über ein Intervall sein, wobei dies in Fig. 3d die Menge 341 ist. Es wird angemerkt, dass sich die Menge 341 mit x ändert, da das Integral über ein Intervall von x genommen wird.

[0094] In Fig. 3d ist die Zunahme gleich $\Gamma(x + s_{fr}) - \Gamma(x)$. Der Gebührenterm kann gleich einem Vielfachen davon sein. Gemäß einer Ausführungsform wird der Wert von $\frac{1}{2}$ verwendet. Es sind andere Optionen möglich.

[0095] Die Menge an Krypto-Token des ersten Typs, um die die Bindungskurve verschoben wird, kann eine Konstante sein. Die Konstante kann, z. B. in dem Smart Contract, festgesetzt sein. Die Konstante kann aktualisierbar sein, wobei z. B. ein Administrator eine Prozedur einer Aktualisierung einer konstanten Verschiebung in dem Smart Contract aufrufen kann. Die Prozedur der Aktualisierung einer konstanten Verschiebung kann konfiguriert sein, eine neue Konstante zu empfangen, oder kann konfiguriert sein, wie im Folgenden angegeben ist, eine neue Konstante zu berechnen. Das Aufrufen der Prozedur kann erfordern, dass in dem Aufruf ein kryptografisches Token, z. B. ein Token, das den Aufrufer authentifiziert, z. B. eine Signatur, enthalten ist.

[0096] Die Menge, um die die Bindungskurve verschoben wird, kann ebenfalls dynamisch berechnet werden. Insbesondere kann sie von dem Register berechnet werden. Zum Beispiel kann der Smart Contract, z. B. die Aktualisierungsprozedur, konfiguriert sein, das Volumen erzeugter und/oder vernichteter Krypto-Token in einer Anzahl neuester Blöcke in dem verteilten Register zu berechnen. Die Menge kann aus dem Volumen berechnet werden. Zum Beispiel kann sie ein Vielfaches davon sein. Die Menge kann gleich dem Volumen sein. Zum Beispiel kann die Menge das Volumen über die letzten sechs Stunden sein oder kann sie die Hälfte des Volumens über die letzten 12 Stunden sein usw. Die zu berücksichtigende Größe des Registers kann in der Zeit ausgedrückt werden, kann aber ebenfalls in Blöcken ausgedrückt werden. Zum Beispiel ist es unwahrscheinlich, dass ein Angriff eine Transaktion in mehr als n Blöcken, wobei n nicht größer als 2 oder 3 gewählt werden kann, beeinflussen kann. Das Volumen kann dann aus cn Blöcken berechnet werden, wobei

c ein Sicherheitsparameter ist, der z. B. 1 oder 2 sein kann. Zum Beispiel ist gemäß einer Ausführungsform die verschobene Menge die Menge an Token, die bei der Erzeugung einer Vernichtungstransaktion in den letzten 4 Blöcken in dem Register getauscht werden. Falls es in dem Register weniger als 4 Blöcke gibt, kann der Smart Contract für die Menge einen Standardwert verwenden.

[0097] Die Bestimmung der Verschiebungsmenge s_{fr} kann vor jeder Erzeugungs- oder Vernichtungsprozedur oder periodisch, z. B. täglich, oder alle m Transaktionen, z. B. alle 100 Transaktionen, erfolgen. Die Bestimmung der Verschiebungsmenge kann z. B. durch einen äußeren Aufruf einer Aktualisierungsprozedur ausgelöst werden. Die Bestimmung der Verschiebungsmenge kann ausgelöst werden, falls in dem Smart Contract definierte Bedingungen erfüllt sind, z. B., falls ein Schwellenwert erfüllt ist; z. B., falls die Anzahl der Transaktionen von Token des ersten Typs einen Schwellenwert übersteigt oder falls die Anzahl von Blöcken in dem Register einen Schwellenwert übersteigt usw.

[0098] Gemäß einer Ausführungsform wird die Erzeugungsfunktion oder eine Vernichtungsfunktion von einer Bindungskurve als eine Linearkombination eines oder mehrerer der Bindungskurve ($\Gamma(x)$), einer verschobenen Bindungskurve ($\Gamma(x + s_{fr})$; $\Gamma(x - s_{fr})$) und einer optionalen Konstante abgeleitet. Es kann mehrere Verschiebungen, z. B. eine Linearkombination von $\Gamma(x)$, $\Gamma(x + s_1)$, $\Gamma(x + s_2)$ und 1, geben.

[0099] Eine Ausführungsform eines computer-implementierten Verfahrens zum Unterhalten von Krypto-Token eines ersten Typs umfasst Folgendes:

- Erhalten eines Smart Contract aus einem verteilten Register, wobei der Smart Contract eine Erzeugungsprozedur zum Erzeugen von Krypto-Token des ersten Typs und eine Vernichtungsprozedur zum Vernichten von Krypto-Token des ersten Typs implementiert, wobei der Smart Contract eine aktuelle Angebotsgröße, die eine aktuelle Anzahl von Krypto-Token des ersten Typs angibt, und eine Bindungskurve, die eine Funktion definiert, unterhält,
- in Ansprechen auf das Initiieren der Kaufprozedur, Berechnen einer Menge von Krypto-Token des zweiten Typs durch Integrieren einer Erzeugungsfunktion von der aktuellen Angebotsgröße bis zu dem aktuellen Angebot plus einer Erzeugungsmenge von Krypto-Token des ersten Typs, Übertragen der Menge von Krypto-Token des zweiten Typs zu einem dem Smart Contract zugeordneten Pool und Erhöhen der aktuellen Angebotsgröße um die Menge von Krypto-Token des ersten Typs und Übertragen der Menge von Krypto-Token des ersten Typs, und
- in Ansprechen auf das Initiieren der Kaufprozedur, Berechnen einer Menge von Krypto-Token des ersten Typs durch Integrieren einer Vernichtungsfunktion von der aktuellen Angebotsgröße bis zu dem aktuellen Angebot minus einer Vernichtungsmenge von Krypto-Token des zweiten Typs, Übertragen der Menge von Krypto-Token des zweiten Typs von dem dem Smart Contract zugeordneten Pool und Verrin-
gern der aktuellen Angebotsgröße um die Menge von Krypto-

[0100] Token des ersten Typs und Ungültigmachen der Menge von Krypto-Token des ersten Typs, wobei

- wenigstens eines der Folgenden zutrifft:
- die Kauffunktion ist eine Summe der Bindungskurve und eines oder mehrerer weiterer Terme einschließlich eines positiven Gebührenterms, und
- die Verkaufsfunktion ist eine Summe der Bindungskurve und eines oder mehrerer weiterer Terme, einschließlich eines negativen Gebührenterms, wobei
- der Gebührenterm eine Summe wenigstens eines Terms ist, der ein Mehrfaches der verschobenen Bindungskurve umfasst.

[0101] Der Gebührenterm kann z. B. eine Differenz zwischen der Bindungskurve und einer Verschiebung der Bindungskurve um einen Wert s_{fr} umfassen.

[0102] Fig. 4a zeigt schematisch ein Beispiel einer Ausführungsform der Aktualisierung einer Bindungskurve. Es kann mehrere Gründe geben, weshalb eine Bindungskurve geändert werden muss, nachdem der Smart Contract definiert worden ist. Ein typischer Grund ist, dass sich die Menge von Krypto-Token in dem zweiten Pool geändert hat und nicht gleich der Menge von Krypto-Token ist, die durch das Integral der Bindungskurve angegeben wird.

[0103] Zum Beispiel kann der Market Maker in einem Zwei-Bindungskurven-System, in dem z. B. die Erzeugung für den Market Maker mehr Token als Vernichtungskosten gewinnt, allmählich mehr Token des zweiten Typs verfügbar haben, als das Integral der Bindungskurve repräsentiert.

[0104] Die Token des zweiten Typs, die durch eine Kauf-Verkaufs-Marge zugewachsen sind, können durch den Market Maker, z. B. in demselben Wallet wie der Pool oder in einem getrennten Wallet, gesammelt werden. Falls alle oder ein Teil der zusätzlichen Token zu dem Pool hinzugefügt werden, kann das Integral der Bindungskurve niedriger als der neue Betrag in dem Pool sein.

[0105] In einer typischen Ausführungsform widerspiegelt der Pool-Saldo immer, wenigstens einmal in der Operation und/oder beim allgemeinen Handel, z. B. im Regime III, den Integralwert. Die Aktualisierungsprozedur kann die Bindungskurve in der Weise ändern, dass das neue Integral den neuen Pool-Saldo angibt, z. B. ihm gleich ist. Der Market Maker kann z. B. in der Weise konstruiert sein, dass der Integralwert und der Pool-Saldo nie verschieden sein können; so dass dementsprechend nur beide zusammen aktualisiert werden.

[0106] Die Token des zweiten Typs, die durch eine Kauf-Verkaufs-Marge zugewachsen sind, können durch den Market Maker z. B. in demselben Wallet wie der Pool gesammelt werden. Der Market Maker kann z. B. ein Wallet besitzen, von dem eine Teilmenge den Pool-Saldo hält, der, z. B., nachdem das System im allgemeinen Betrieb ist, genau das Integral widerspiegeln kann. Eine zweite Teilmenge des Wallets des Market Makers könnte weiteren Wert, z. B. ein durch den Market Maker erzeugtes Einkommen, halten. In diesem Fall kann der Wert des Wallets von dem Integral und von dem Pool-Saldo verschieden sein, obwohl die beiden Letzteren ideal ausgeglichen sein können. Zum Beispiel kann das Ändern des Pool-Saldos dadurch erfolgen, dass eine Aktualisierungsprozedur aufgerufen wird, die den Pool-Saldo und die Kurvenform zusammen anpassen würde, wobei sie einen Wert zu und von dem Pool-Saldoteil des Wallets überträgt. Der Pool-Saldo kann als eine durch das Integral der Bindungskurve, z. B. durch das Integral von dem Angebot null bis zu dem aktuellen Angebot, angegebene Menge definiert sein. Gemäß einer Ausführungsform ist sichergestellt, dass die Menge des Wallet mindestens so hoch ist, wie das Integral angibt.

[0107] Die Token des zweiten Typs, die durch eine Kauf-Verkaufs-Marge zugewachsen sind, können ebenfalls oder stattdessen getrennt gesammelt werden. Zum Beispiel ist eine Erzeugungsfunktion höher als die Vernichtungsfunktion. Der Überschuss kann für jede Erzeugungstransaktion gesammelt werden. Zum Beispiel kann ein zweiter Pool, z. B. ein zweites Wallet des Market Makers, die Gebühren sammeln. An einem Punkt können die Gebühren in dem zweiten Pool oder ein Teil davon zu dem ersten Pool addiert werden. In diesem Fall wird der Pool größer, als das Integral der Bindungskurve nahelegt, was durch Neuanpassen der Bindungskurve korrigiert werden kann.

[0108] In **Fig. 4a** ist eine Bindungskurve als eine durchgezogene Linie und eine aktualisierte Kurve als die Strichlinie gezeigt.

[0109] Das Aktualisieren einer Bindungskurve kann demselben Prozess wie das Auswählen der Anfangsbindungskurve für den Anfangs-Smart-Contract folgen. Gemäß einer Ausführungsform wird eine Parameterdarstellung der Kurvensegmente gewählt. Zum Beispiel können die Parameter für ein Segment, zwischen welchen Angebotspunkten ein Kurvensegment gültig ist, z. B. von 0 bis s_1 , von s_1 bis s_2 usw., und Koeffizienten einer Gleichung, die die Kurve definiert, sein. Die Beschränkungen können von drei Arten sein.

[0110] Gemäß einer Ausführungsform erlegen die Beschränkungen den Parametern lineare Beziehungen auf. Ein Vorteil ist, dass das Anpassen oder Neuanpassen (Aktualisieren) der Bindungskurve das Lösen eines linearen Gleichungssystems umfasst. Dies kann selbst in der Chain preiswert erfolgen. Unter der Annahme, dass die x-Koordinate des Anfangs des Segments festgesetzt ist und nicht angepasst wird, können selbst exponentielle Terms durch lineare Gleichungen angepasst werden.

[0111] Die aktualisierte Bindungskurve weist neue Parameter auf. In **Fig. 4a** sind diese als Parameter 324, 325 und 326 gezeigt. Zufällig ist die Anzahl der Parameter in diesem Beispiel dieselbe, obwohl die Anzahl der Segmente ebenfalls geändert sein kann.

[0112] Das Aktualisieren der Bindungskurve oder Bindungskurven kann durch Aufrufen einer Aktualisierungsprozedur 223 initiiert werden. Aus Sicherheitsgründen kann die Aktualisierungsprozedur auf bestimmte Aufrufer, z. B. Regulatoren [engl.: „governors“] des Vertrags, beschränkt sein. Alternativ kann die Aktualisierung z. B. automatisch ausgelöst werden, sobald ein zweiter Pool einen vorgegebenen Wert übersteigt.

[0113] Es kann mehr als eine Aktualisierungsprozedur geben. Die obige Aktualisierungsprozedur kann verwendet werden, um die Bindungskurve an eine Pool-Menge anzupassen. Allerdings kann eine Aktualisierungsprozedur ebenfalls für das Regulieren verwendet werden. Dies könnte eine andere Prozedur, z. B. eine zweite Aktualisierungsprozedur, sein. Zum Beispiel kann sich herausstellen, dass die Bindungskurve an einigen Stellen zu steil oder nicht steil genug ist. Es kann dann eine Aktualisierungsprozedur aufgerufen werden, um die Beschränkungen zu aktualisieren und die Kurve neu anzupassen.

[0114] Gemäß einer Ausführungsform implementiert der Smart Contract eine Aktualisierungsprozedur zum Aktualisieren der Bindungskurve. Die Aktualisierungsprozedur kann das Anpassen eines oder mehrerer Kurvensegmente an eine oder mehrere Beschränkungen umfassen. Die Beschränkungen können die Beschränkung umfassen, dass das Integral über eine Vernichtungsfunktion, die von der aktualisierten zweiten Bindungskurve abgeleitet ist, bis zu der aktuellen Angebotsgröße kleiner oder gleich der Menge der Krypto-Token des zweiten Typs in dem Pool ist. Das Integral kann von 0 bis zu der aktuellen Angebotsgröße berechnet werden.

[0115] Ein Verfahren kann das Übertragen einer zusätzlichen Menge von Krypto-Token des zweiten Typs an den Pool umfassen, wobei das Integral über die aktualisierte zweite Bindungskurve kleiner oder gleich der neuen Pool-Menge ist. Diese Übertragung kann unabhängig von der Aktualisierung erfolgen oder in der Aktualisierungsprozedur ausgeführt werden oder durch die Aktualisierungsprozedur überprüft werden.

[0116] Falls Kurvensegmente verwendet werden, um die Bindungskurve zu definieren, kann die Aktualisierungsprozedur die Anzahl mehrerer Kurvensegmente erhöhen oder verringern.

[0117] **Fig. 4b** zeigt schematisch ein Beispiel einer Ausführungsform einer Bindungskurve. Die in **Fig. 4b** gezeigte Bindungskurve ist als eine Folge von Kurvensegmenten definiert. Es sind drei Segmente gezeigt: Γ_0 , Γ_1 und Γ_2 . Es könnte zwei Segmente oder mehr als drei Segmente geben. Die y-Koordinate des Anfangspunkts jedes Segments ist durch P_0 , P_1 und P_2 bezeichnet. Es wird angemerkt, dass P_i eine Menge von Token des zweiten Typs angibt, obwohl sie in **Fig. 4b** auf der x-Achse gezeigt sind. Die Zunahmen der entsprechenden x-Koordinaten sind durch Δx_0 und Δx_1 bezeichnet. Es wird angemerkt, dass die P_0 entsprechende x-Koordinate null ist.

[0118] Gemäß einer Ausführungsform sind die Kurvensegmente durch Polynome definiert, wobei z. B. ein Polynom eine x-Koordinate auf eine y-Koordinate abbildet. Es ist zweckmäßig, die Polynome als eine Bezier-Kurve zu schreiben. Als eine vorteilhafte Wahl stellen sich kubische Bézier-Kurven heraus. Um eine kubische Bezier-Kurve über aufeinanderfolgende Punkte P_i anzupassen, kann die folgende Formel verwendet werden. Die Werte a_i und b_i sind zusätzlich, um die Kurve anzupassen.

$$\Gamma_i(t) = (1-t)^3 \cdot P_i + 3t(1-t)^2 \cdot a_i + 3t^2(1-t) \cdot b_i + t \cdot P_{i+1}.$$

[0119] Um die Kurven anzupassen, können verschiedene Bedingungen auferlegt werden. Zunächst können eine stetige erste und zweite Ableitung an den Verbindungspunkten gefordert werden. Unter Berücksichtigung dessen, dass die Ableitung nach t ist, ergibt sich Folgendes:

$$\Gamma'_{i-1}(t=1) \frac{\Delta x_i}{\Delta x_i - 1} = \Gamma'_i(t=0)$$

$$\Gamma''_{i-1}(t=1) \frac{\Delta x_i}{\Delta x_i - 1} = \Gamma''_i(t=0).$$

[0120] Dementsprechend ergibt sich

$$\Gamma'_i = 3 \left[-(1-t)^2 \cdot P_i + (1-3t)(1-t) \cdot a_i + t(2-3t) \cdot b_i + t^2 \cdot P_{i+1} \right]$$

und

$$\Gamma''_i = 6 \left[(1-t) \cdot P_i + (3t-2) \cdot a_i + (1-3t) \cdot b_i + t \cdot P_{i+1} \right].$$

[0121] Bei den Verbindungspunkten bedeutet dies:

$$\Gamma_i'(t=0) = 3(-P_i - a_i)$$

$$\Gamma_i'(t=1) = 3(-b_i + P_{i+1})$$

$$\Gamma_i''(t=0) = 6(-P_i - 2a_i + b_i)$$

$$\Gamma_i''(t=1) = 6(a_i - 2 \cdot b_i + P_{i+1}).$$

[0122] Um die Kurve auf einen neuen Pool-Saldo zu aktualisieren (auch als Unterfüttern [engl.: „undergirding“] bezeichnet), wird die Kurve Γ_i integriert. Um dies in Parameterform zu tun, aber die richtige Fläche auszulesen, muss die Substitution beachtet werden, wobei x der aktuelle Angebotspunkt ist. Dabei wird angenommen, dass x zwischen x_i und x_{i+1} liegt.

$$\frac{x - x_i}{x_{i+1} - x_i} = t$$

$$\frac{dx}{dx} = \frac{1}{x_{i+1} - x_i} = \frac{1}{\Delta x_i}$$

$$\rightarrow dx = \Delta x_i \cdot dt$$

[0123] Da Δx_i während der Integration konstant (keine Funktion von x) ist, kann es herausgezogen werden, so dass Folgendes gilt

$$\int \Gamma_i(x) dx = \Delta x_i \cdot \int \Gamma_i(t) dt$$

$$\Delta x_i \cdot \int \Gamma_i(t) dt = \Delta x_i \cdot \frac{1}{4} \left[(-t^4 + 4t^3 - 6t^2 + 4t) \cdot P_i + (3t^4 - 8t + 6t) \cdot a_i - (3t^4 - 4t^3) \cdot b_i + t \cdot 4P_{i+1} \right] + C.$$

[0124] Für das vollständige Kurvenabschnittsintegral ergibt sich:

$$\Delta x_i \int_0^1 \Gamma_i(t) dt = \Delta x_i \cdot \frac{1}{4} (a_i + b_i + P_{i+1} + P_i)$$

und für das partielle Integral:

$$\Delta x_i \cdot \int_0^{\tilde{t}} \Gamma_i(t) dt = \Delta x_i \cdot \frac{1}{4} \left[(-\tilde{t}^4 + 4\tilde{t}^3 - 6\tilde{t}^2 + 4\tilde{t}) \cdot P_i + (3\tilde{t}^4 - 8\tilde{t} + 6\tilde{t}) \cdot a_i - (3\tilde{t}^4 - 4\tilde{t}^3) \cdot b_i + \tilde{t} \cdot 4P_{i+1} \right].$$

[0125] Falls der aktuelle Angebotspunkt innerhalb des Segments I liegt, wird das Teilintegral dort gelöst. Andernfalls kann für die folgenden anderen Segmente die volle Integralgleichung ($0 \rightarrow t \rightarrow 1$) verwendet werden, die nicht von x , sondern nur von Δx abhängt.

[0126] Das Aktualisieren einer Bindungskurve kann die Anzahl mehrerer Kurvensegmente erhöhen oder verringern. Außerdem kann hier die Pool-Saldo-Bedingung als eine Anforderung für die Bindungskurve verwendet werden. Das heißt, das Integral über die Kurve bis zu dem aktuellen Angebot sollte der aktuellen Pool-Größe entsprechen, z. B. ihr gleich oder ein Prozentsatz usw. sein.

[0127] Im Folgenden sind weitere Einzelheiten, Optionen und Ausführungsformen, insbesondere hinsichtlich Gegenmaßnahmen gegen Frontrunning-Angriffe, dargestellt. Ohne Verluste der Allgemeinheit konzentriert sich das Folgende auf die Erzeugungsseite, z. B. auf die Kaufseite. Die Vernichtungsseite, z. B. die Verkaufsseite, kann analog behandelt werden.

[0128] Es wird angenommen, dass ein Benutzer eine normale Kaufbestellung τ_1 für eine Menge des Angebots s_1 mit einem möglicherweise durch I_1 beschränkten mittleren Preis verbucht:

$$\tau_1^b : \text{Kauf}, s_1, l_1.$$

[0129] Ein Frontrunning dieser Kauftransaktion würde erfordern, dass ein Angreifer zwei Transaktionen direkt vor und nach τ_1 platziert, d. h.

$$\tau_0^b : \text{Kauf}, s_0$$

$$\tau_2^s : \text{Verkauf}, s_2 \text{ mit } s_2 = s_0.$$

[0130] Es wird angemerkt, dass die Differenz $|s_1 - s_2|$ nicht Teil des Angriffs ist, falls der Angreifer weniger verkauft, als er gekauft hat. Dasselbe gilt in dem Fall, dass er mehr verkauft, als er unmittelbar vor τ_1 gekauft hat.

[0131] Es wird angenommen, dass der aktuelle Betriebspunkt bei $(\tilde{p}, \tilde{s})$ eingestellt ist und dass der Kauf und Verkauf wie folgt gegeben sind:

$$p_s = p - \sigma_{p,s}$$

$$p_b = p + \sigma_{p,b},$$

wobei p der Referenzpreis des Bindungskurven-Modells $\Gamma(x)$ ist und die Kauf- und Verkaufsmarge $\sigma_{p,b}$ bzw. $\sigma_{p,s}$, sind.

[0132] Wenn die Transaktionskosten c aufgenommen werden und das Pool-Saldo-Integral verwendet wird, ist der Wert, der für eine Kauftransaktion zu zahlen ist und für eine Verkaufstransaktion zurückgegeben wird, als $p_s = p - \sigma_{p,s}$ und $p_b = p + \sigma_{p,b}$ gegeben.

[0133] Es wird angemerkt, dass die Gebühr σ_p in diesem Fall eine Funktion von x ist und somit innerhalb des Integrals liegt. Andere Gebührenbeiträge wie etwa die dynamische Gebühr, die auf dem Handelsverlauf beruht, könnten unabhängig sein und vergleichbar mit den Handelskosten aus dem Integral herausgezogen werden:

$$v_{\tau_i^b} = \int_{\tilde{s}}^{\tilde{s}+s_b} \Gamma(x) + \sigma_{p,b} dx + c_{\tau_i^b} \quad (73)$$

$$v_{\tau_i^s} = \int_{\tilde{s}-s_s}^{\tilde{s}} \Gamma(x) + \sigma_{p,s} dx + c_{\tau_i^s}. \quad (74)$$

[0134] Wegen eines hochfrequenten Frontrunning-Angriffs überzahlt der Benutzer:

$$v_{ov} = \int_{\tilde{s}+s_0}^{\tilde{s}+s_0+s_1} \Gamma(x) + \sigma_{p,b} dx - \int_{\tilde{s}}^{\tilde{s}+s_1} \Gamma(x) + \sigma_{p,b} dx, \quad (75)$$

während der Ertrag und die Rendite des Angreifers wie folgt sind:

$$v_{\tau_2^s} - v_{\tau_0^b} = \int_{\tilde{s}+s_1}^{\tilde{s}+s_0+s_1} \Gamma(x) - \sigma_{p,s} dx - c_{\tau_i^s} - \int_{\tilde{s}}^{\tilde{s}+s_0} \Gamma(x) + \sigma_{p,b} dx - c_{\tau_i^s} \quad (76)$$

$$R_{\text{Angriff}} = \frac{v_{\tau_2^s} - v_{\tau_0^b}}{v_{\tau_0^b}}. \quad (77)$$

[0135] Das Ziel der Kauf/Verkaufs-Marge σ ist es entweder, den Ertrag des Angreifers zu null oder negativ zu machen, z. B., dass der Angreifer mehr zahlt, als er gewinnt, oder wenigstens die Rendite geeignet zu minimieren. In modernen verteilten Registersystemen sind Transaktionskosten in Bezug auf den tatsächlichen Handelswert, insbesondere, falls der Angreifer ein Miner ist, der zu verringerten Kosten Zugang zu der Transaktionsausführung haben könnte, häufig vernachlässigbar. Somit werden Transaktionskosten hier in den folgenden Ableitungen vernachlässigt, um auf der sicheren Seite zu sein, so dass die Angriffsverhinderung selbst bei Transaktionskosten von null wirksam ist.

[0136] Es wird angemerkt, dass für typische Bindungskurven der Anstieg > 0 ist, so dass der Wert mit s_0 zunimmt. Somit kann ein Angreifer τ_1 in ein Gebiet mit maximalem Anstieg verschieben, da sich seine Ertragsrate erhöhen würde. Eine naive Vorgehensweise wäre, eine konstante Margenfunktion, z. B. eine Gebühr auf der Grundlage eines Prozentsatzes des Handelsvolumens, einzuführen, die so definiert ist, dass die Verschiebung zu dem steilsten Gebiet wirtschaftlich ineffizient wäre. Allerdings ist die geforderte Verschiebungsbreite klein, der Gewinn aber groß, wenn der Handelspunkt in der Nähe des steilen Gebiets ist. Eine angemessene Gebühr, um diesen Situationen entgegenzuwirken, würde jeden normalen Benutzer eine ungerechtfertigt hohe Menge einer Gebühr zahlen lassen, wenn er in weniger steilen Gebieten der Kurve handelt.

[0137] Eine Untersuchung der Gleichungen, insbesondere von Gleichung 76, zeigt allerdings, dass ein natives Erzwingen von $v_{\tau_2^s} - v_{\tau_0^b} \leq 0$ einerseits den Angriff unwirksam machen würde. Andererseits würde es ebenfalls irgendeinen Gewinn von dem späteren Verkauf früher gekaufter Token entfernen, was allerdings unerwünscht wäre. Gemäß einer Ausführungsform wird ein Gebührenmodell verwendet, das von lokalen Eigenschaften der Kurve, z. B. einem Gebiet um die aktuelle Angebotsgröße, abhängt. Die Margenterme sollten den Wertgewinn von einer Aufwärtsverschiebung in Bezug auf einen früheren Kauf im Fall eines späteren Verkaufs bzw. einer Abwärtsverschiebung in Bezug auf einen früheren Verkauf für den späteren Kauf entfernen und dadurch Kauf/Verkaufs-Frontrunning-Angriffe effektiv unwirksam machen, während sie einen Wertgewinn wegen Zwischentransaktionen anderer Benutzer zulassen.

[0138] Diese Probleme könnten dadurch gemildert werden, dass das Frontrunning bis zu einem bestimmten Volumen ineffizient gemacht wird. Die Grundeinsicht ist, dass eine hf-Frontrunning-Verhinderung andererseits und Zulassen des gewöhnlichen Handels andererseits dadurch möglich sind, dass ein Referenzbetrag (im Folgenden s_{fr}) eingeführt wird und dass verhindert wird, dass sich Gewinne für das hf-Frontrunning aller Handel auf gleich oder weniger als diese Menge summieren, während Gewinne für zwei beliebige Handel, die eine größere Menge des Angebots einklammern, möglich sind. Dies wird im Folgenden dargestellt.

[0139] Zunächst wird eine Menge des Angebots als Referenzangebot für die Frontrunning-Verhinderung definiert:

s_{fr} Frontrunning - Verhinderungs - Angebotsmenge. (78)

[0140] Gemäß einer Ausführungsform kann das Gebührenmodell wie folgt auf den Preis einwirken:

$$\sigma^{gfr} = \frac{1}{2} \cdot \begin{cases} \Gamma(x + s_{fr}) - \Gamma(x) & \text{Kauf} \triangleq \sigma_{p,b} \\ \Gamma(x) - \Gamma(x - s_{fr}) & \text{Verkauf} \triangleq \sigma_{p,s} \end{cases} \quad (79)$$

[0141] In einer anderen Ausführungsform, z. B. in einer symmetrischen Vorgehensweise, können die Gebühren wie folgt sein, um die Kosten nur auf der Verkaufsseite aufzuerlegen; wobei die Vorgehensweise für die Kaufseite ähnlich ist:

$$\sigma^{gfr} = \begin{cases} 0 & \text{Kauf} \triangleq \sigma_{p,b} \\ \Gamma(x) - \Gamma(x - s_{fr}) & \text{Verkauf} \triangleq \sigma_{p,s} \end{cases} \quad (80)$$

[0142] In dem symmetrischen Fall ist die Reihenfolge der Subtraktion für die Kauf- und für die Verkaufsseite verschieden, da die Kurve $\Gamma(x)$ streng wächst und da die Definition von (73, 74) für σ_p positiv ist. Die Anwendung der asymmetrischen Vorgehensweise ist z. B. nützlich für ein System, bei dem das Kaufen kleine Gebühren haben sollte, um das Teilnehmen effizient zu machen, während zugelassen ist, dass das Ausgeben der Token im Vergleich zu ihrem Verkaufen privilegierter ist.

[0143] Die Kauf- und Verkaufswertgleichungen (74, 73) können (unter Vernachlässigung von Transaktionskosten, aus den oben diskutierten Gründen) wie folgt geschrieben werden:

symmetrischer Fall:

$$v_{\tau_i^b} = \int_{\bar{s}}^{\bar{s}+s_b} \Gamma(x) - \frac{1}{2} (\Gamma(x) - \Gamma(x + s_{fr})) dx \quad (81)$$

$$= \int_{\tilde{s}}^{\tilde{s}+s_b} \Gamma(x) + \frac{1}{2} \Gamma(x) - \Gamma(x + s_{fr}) dx \quad (82)$$

$$v_{\tau_i^s} = \int_{\tilde{s}-s_s}^{\tilde{s}} \Gamma(x) - \frac{1}{2} (\Gamma(x) - \Gamma(x - s_{fr})) dx \quad (83)$$

$$= \int_{\tilde{s}-s_s}^{\tilde{s}} \frac{1}{2} \Gamma(x) + \frac{1}{2} \Gamma(x - s_{fr}) dx. \quad (84)$$

asymmetrischer Fall der Verkaufsseite:

$$v_{\tau_i^b} = \int_{\tilde{s}}^{\tilde{s}+s_b} \Gamma(x) dx \quad (85)$$

$$v_{\tau_i^s} = \int_{\tilde{s}-s_s}^{\tilde{s}} \Gamma(x) - (\Gamma(x) - \Gamma(x - s_{fr})) dx \quad (86) \quad (87)$$

$$= \int_{\tilde{s}-s_s}^{\tilde{s}} \Gamma(x - s_{fr}) dx. \quad (88)$$

[0144] Ein allgemeiner hffr-Angriff könnte aus einer beliebigen Folge von Kauftransaktionen und späteren Verkaufstransaktionen (oder im Fall von Verkaufs-Fronrunning, Verkaufs- und späteren Kauftransaktionen) gebildet werden, die sich bis zu einer Gesamtmenge s_a aufsummieren:

$$s_a = \sum_{i=0}^n s_{a,i}.$$

[0145] Ohne Verlust der Allgemeinheit können diese wie im Folgenden für den symmetrischen Kauf-Fall dargestellt summiert werden:

$$\begin{aligned} v_{\tau_i^b} &= \frac{1}{2} \left[\int_{\tilde{s}}^{\tilde{s}+s_{a,0}} \Gamma(x) + \Gamma(x + s_{fr}) dx + \dots + \int_{\tilde{s}+s_{a,n-1}}^{\tilde{s}+s_{a,n}} \Gamma(x) + \Gamma(x + s_{fr}) dx \right] \\ &= \frac{1}{2} \cdot \int_{\tilde{s}}^{\tilde{s}+s_a} \Gamma(x) + \Gamma(x + s_{fr}) dx. \end{aligned}$$

[0146] Der asymmetrische Fall und die Verkaufsseite sind dementsprechend.

[0147] Somit ist der Kauf/Verkaufs-Gewinn, wenn ein Satz von Transaktionen, die bis zu s_1 aufsummiert werden:

$$s_1 = \sum_i s_i, \quad (89)$$

durch eine Gesamtangriffsmenge von s_a geklammert wird, wie folgt gegeben:

symmetrischer Fall:

$$v_{\tau_{Angriff}^s} - v_{\tau_{Angriff}^b} = \int_{\tilde{s}+s_1}^{\tilde{s}+s_1+s_a} \frac{1}{2} \Gamma(x) + \frac{1}{2} \Gamma(x - s_{fr}) dx \quad (90)$$

$$- \int_{\tilde{s}}^{\tilde{s}+s_a} \frac{1}{2} \Gamma(x) + \frac{1}{2} \Gamma(x + s_{fr}) dx \quad (91)$$

$$= \frac{1}{2} \cdot \int_{\tilde{s}+s_1}^{\tilde{s}+s_1+s_a} \Gamma(x) - \Gamma(x - s_1 + s_{fr}) + \Gamma(x - s_{fr}) \Gamma(x - s_1) dx. \quad (92)$$

asymmetrischer Fall:

$$v_{\tau_{Angriff}^s} - v_{\tau_{Angriff}^b} = \int_{\tilde{s}+s_1}^{\tilde{s}+s_1+s_a} \Gamma(x - s_{fr}) - \Gamma(x - s_1) dx. \quad (93)$$

[0148] Unabhängig von der Angriffsgröße (oder Angriffsteilfolge) ist der Gewinn für $s_1 = s_{sr}$ null und für $s_1 < s_{sr}$ kleiner als null (was den Angriff somit wirtschaftlich ineffizient macht). Es wird angemerkt, dass diese Gleichungen sowohl für Kaufs als auch für Verkaufsangriffe gelten.

[0149] Die Gebühr für einen normalen Benutzer, der zu demselben Preis kauft und später verkauft - Grenzfall der Gleichungen (92, 93) $s_1 \rightarrow 0$ -, entspricht grundsätzlich der Fläche, die wegen des Anstiegs des Handelsgebiets und der Skalierung mit der gehandelten Menge über s_{fr} gewonnen wird, was das Gewünschte ist. In dem folgenden Abschnitt wird dies veranschaulicht und werden einige Zahlen gegeben.

[0150] Fig. 4c zeigt eine Bindungskurve und stellt als ein Beispiel die asymmetrische Margenfunktion $\sigma_{gr}(80)$ während eines Kauf-Frontrunning-Angriffs mit $s_a = s_{fr}$ dar.

[0151] Fig. 4c stellt den Kauf/Verkauf in der Situation dar, dass es in dem asymmetrischen Fall keine Zwischenhandel gibt. Der Kauf würde die Fläche 1 kosten, allerdings würde der Verkauf die Fläche liefern, wenn mit um $(-s_{fr})$ verschobenen Integrationsgrenzen integriert wird. Die symmetrische Vorgehensweise würde auf jede Seite die Summe der Hälfte der Fläche (Integrationsgrenzen einmal um s_{fr} , einmal um $-s_{fr}$ verschoben) anwenden. Alle anderen Fälle mit gebogenen Kurven, Wendepunkten usw. sind analog.

[0152] Der Kauf geschieht ohne Zusatzgebühr und Zusatzkosten. Die anderen Käufer kaufen um $s_1 = s_{fr}$ auf. Danach verkauft der Angriff $s_2 = s_{fr}$. Ohne Marge würde dies den der Fläche 2 entsprechenden Gewinn liefern, der durch die Margenfunktion entfernt wird, so dass der ausgezahlte Wert 1a genau gleich 1 ist und der Angreifer somit keinen Gewinn hat:

$$v_{\tau_2^s} = \int_{\tilde{s}+s_0}^{\tilde{s}+s_0+s_1} \Gamma(x - s_{fr}) dx = \int_{\tilde{s}}^{\tilde{s}+s_0} \Gamma(x) dx. \quad (94)$$

Fig. 4d zeigt eine Bindungskurve und stellt den Kauf/Verkauf für die Situation ohne Zwischenhandel in dem asymmetrischen Beispiel dar. Der Kauf würde die Fläche 1 kosten, wobei der Verkauf aber die Fläche liefern würde, wenn mit um $(-s_{fr})$ verschobenen Integrationsgrenzen integriert wird. Die symmetrische Vorgehensweise würde auf jede Seite die Summe der Hälfte der Fläche anwenden (Integrationsgrenzen einmal um s_{fr} , einmal um $-s_{fr}$ verschoben). Andere Fälle mit anderen Bindungskurven, z. B. mit gebogenen Kurven, Wendepunkten usw., sind analog.

[0153] Es wird ein tokenisiertes System des Referenzwerts $\bar{v}$, des Referenzpreises $\bar{p}$ und des Token-Angebots $\bar{s}$ angenommen. Der Anstieg um das Referenzangebot sei:

$$\Gamma'(\bar{s}) = \frac{n \cdot \bar{p}}{\bar{s}} \quad (95)$$

und die Frontrunning-Verhinderungsmenge des Angebots:

$$s_{fr} = \frac{\bar{s}}{m}. \quad (96)$$

[0154] Es wird angenommen, dass die Krümmung vernachlässigbar ist; da die Gebühr durch den Anstieg, nicht durch die Krümmung dominiert ist, ist dies eine sinnvolle Annahme. Die Funktion (die 1. zwei Terme der Taylor-Entwicklung um $\bar{s}$) kann dann wie folgt geschätzt werden:

$$\Gamma(x, \bar{s}) = \Gamma(\bar{s}) + \Gamma'(\bar{s}) \cdot (x - \bar{s}). \quad (97)$$

[0155] Einsetzen in die Gewinngleichungen für $s_1 = 0$ und $\tilde{s} = \bar{s}$ liefert:

$$\begin{aligned} \frac{|v_{Gebühr}|}{v_{Handel}} &= \frac{\left| \int_{\bar{s}-\frac{1}{2}s_a}^{\bar{s}+\frac{1}{2}s_a} \Gamma(x - s_{fr}) - \Gamma(x) dx \right|}{\bar{p} \cdot s_a} \\ &= \frac{s_{sf} \cdot \Gamma'(\bar{s}) \cdot s_a}{\bar{p} \cdot s_a} \\ &= \frac{n}{m}. \end{aligned}$$

[0156] Falls nun gefordert wird, dass die Gesamtgebühr die üblichen 1 % (Kauf und Verkauf zusammen) ist, ergibt sich:

$$m = \frac{n}{100},$$

d. h. für das konkrete Beispiel $s_{fr} \approx \frac{1}{33} \bar{s}$. Tatsächlich würde ein viel kleinerer Faktor $\left(\approx \frac{1}{1000}\right)$ verwendet, was ermöglichen würde, dass die Margengebühr $\approx \frac{1}{30} \%$ wäre.

[0157] Ein zensurbasiertes Frontrunning (cfr) erfordert ein geheimes Einverständnis unter einem größeren Teil der Miner. Ein Beispiel wäre das Platzieren einer Kauftransaktion, daraufhin das Sperren der gesamten Verkaufstransaktion und nur das Zulassen von Kauftransaktionen, schließlich das Verkaufen und somit das Extrahieren des Werts vor der Verarbeitung der gesammelten Verkaufstransaktionen.

[0158] Neben diesen Kauf/Verkaufs-Frontrunning-Angriffen, bei denen das Handelspaar (Kauf und Verkauf) speziell angeordnet wird, um andere Transaktionen einzuklammern, gibt es auch andere zensurbasierte Angriffe. Ein Beispiel wäre der Fall des geheimen Einverständnisses von Minern oder Benutzern in Bezug auf das geheime Einverständnis von Minern, die sich bereits entschieden haben, zu kaufen (oder verkaufen), wobei die Transaktion, z. B. durch Neusortieren der Transaktionen vor der Ausführung, z. B. dadurch, dass zunächst Verkaufstransaktionen, daraufhin die privilegierte Kauftransaktion, daraufhin andere Kauftransaktionen ausgeführt werden, privilegiert, z. B. mit Priorität behandelt, werden könnte. Die vorliegende dynamische Kauf-Verkaufs-Marge wirkt diesem bereits entgegen, so dass Kauf- und Verkaufstransaktionen für einen einstellbaren Zeitrahmen entkoppelt sind.

[0159] Im Folgenden werden Mittel bereitgestellt, um dem ersten Typ von Angriffen (Einklammern) entgegenzuwirken. Die Vorgehensweise kann verwendet werden, um einen Angriff auf der Grundlage einer einseitigen Zensur auf Kauf- und Verkaufstransaktionen zu behandeln.

[0160] Es wird angenommen, dass es eine Menge von im geheimen Einverständnis stehenden Minern gibt, die in der Lage sind, Kauf- und Verkaufstransaktionen zu verzögern. Diese Transaktionen werden a) in den Transaktions-Pool nicht akzeptiert oder b) obwohl sie in dem Transaktions-Pool sind, vor der Ausführung wenigstens eine bestimmte Zeitdauer ignoriert. Die Anwendung der Kauf-Verkaufs-Marge σ_{gr} auf der Grundlage der Angebotsmenge (79, 80) macht diese Art eines Angriffs wirtschaftlich ineffizient. Allerdings könnten im geheimen Einverständnis stehende Miner im Gegensatz zu normalen Benutzern Transaktionen in der Weise verzögern und neu sortieren, dass das zu handelnde Volumen in dem Pool nicht ausgeführter Transaktionen über die Menge s_{fr} , für die das Frontrunning wirtschaftlich ineffizient wäre, wächst.

$$s_{Pool}^b = s_{fr} + \Delta_{Kauf} \quad (98)$$

$$s_{Pool}^s = s_{fr} + \Delta_{Verkauf} \quad (99)$$

[0161] Zum Beispiel könnte ein Kaufseitenangriff s_{Pool}^s verzögern, da der Anstieg üblicherweise mit s zunimmt und es vorteilhafter ist, den Angriff auf einem höheren Gesamtangebot zu halten. Daraufhin wird ihr eigener Kauf platziert, s_{Pool}^b ausgeführt und schließlich erneut verkauft. Dadurch kann ein Gewinn proportional zu Δ_{Kauf} bzw. $\Delta_{Verkauf}$ extrahiert werden. Die Gleichungen (76, 77) können dementsprechend angewendet werden.

[0162] Diese Art des Angriffs kann dadurch gemildert werden, dass s_{fr} in Bezug auf das mittlere Handelsvolumen und den Zeitpunkt gewählt wird. Wie oben diskutiert wurde, kann s_{fr} in der Weise gewählt werden, dass die zugehörigen Gebühren akzeptabel sind. Obwohl s_{fr} unabhängig von den zeitbasierten Informationen ist, ist aber interessant, dass es über den Fluss des gehandelten Angebots mit einem Zeitrahmen zusammenhängen kann. Zum Beispiel kann der Fluss des gehandelten Angebots verwendet werden:

$$\dot{s}_{gehandelt} = \frac{\partial s_{gehandelt}}{\partial t} \quad (100)$$

[0163] Falls ein Angreifer eine größere Angebotsmenge als s_{fr} einklammert - um in der Lage zu sein, einen Gewinn zu extrahieren, müsste bis zu

$$t_{\text{Warten}} = \frac{s_{fr}}{\dot{s}_{\text{gehandelt}}} \quad (101)$$

gewartet werden.

[0164] Zum Vergleich ist das täglich gehandelte Angebot in Bitcoin üblicherweise um $\frac{1}{4}\%$. Dieses enthält alle Kauf- und Verkaufstransaktionen. In einer einfachen Näherung könnte somit angenommen werden, dass das täglich gehandelte Angebot entweder für den Kauf oder für den Verkauf $\approx \frac{1}{8}\%$ ist. Allerdings kann sich dies in Kauf- oder Verkaufsschüben ändern. Dies ist im Folgenden weiter diskutiert. Gemäß einer Ausführungsform könnte somit angenommen werden, dass das gehandelte Angebot zu normalen Zeiten üblicherweise weit unter $\frac{1}{10}\% / 24h$ liegt. Die Wartezeit könnte wie folgt genähert werden:

$$s_{fr} = \frac{1}{2000} \bar{s} \leftrightarrow t_{\text{Warten}} \approx 12h \quad (102)$$

$$s_{fr} = \frac{1}{2000} \bar{s} \leftrightarrow t_{\text{Warten}} \approx 6h. \quad (103)$$

[0165] Gemäß einer Ausführungsform wird eine dynamische Anpassung von s_{fr} auf der Grundlage des aktuellen oder früheren s -Flusses (z. B. des Mittelwerts über die letzten n Stunden) eingeführt. Diese Erweiterung, die Handelsflussschüben entgegenwirkt, könnte t_{Warten} zu klein machen. Somit würde s_{fr} z. B. in Schritten oder kontinuierlich erhöht, falls die Referenzvariable, z. B. der mittlere Fluss in den letzten n Stunden, größer als bestimmte Werte würde.

[0166] Zum Beispiel kann s_{fr} von dem Handelsvolumen in/über einen früheren Zeitrahmen, z. B. eine frühere Anzahl von Stunden, abgeleitet werden. Das Handelsvolumen kann ebenfalls als das Handelsvolumen in einer früheren Anzahl von Blöcken genommen werden. Ebenso kann es von dem Register, wie es z. B. für den Miner verfügbar ist, abgeleitet werden. Zum Beispiel kann s_{fr} ein Vielfaches des Handelsvolumens, z. B. die Hälfte des Volumens in den letzten 6 Blöcken, sein. Der Wert kann auf der Grundlage der beobachteten früheren Handelsvolumina und des geforderten Widerstands gegen einen Angriff, z. B. eines Widerstands gegen ein bestimmtes Niveau von gegenseitigem Einverständnis der Miner, z. B. eines gegenseitigen Einverständnisses von 10 %, experimentell festgesetzt werden.

[0167] Fig. 5 zeigt schematisch ein Beispiel einer Ausführungsform eines Verfahrens 500 zum Unterhalten von Krypto-Token eines ersten Typs. Das Verfahren 500 ist computer-implementiert und umfasst:

- Erhalten (510) eines Smart Contract von einem verteilten Register, wobei der Smart Contract eine Erzeugungsprozedur zum Erzeugen von Krypto-Token des ersten Typs im Tausch gegen Krypto-Token des zweiten Typs und eine Vernichtungsprozedur zum Vernichten von Krypto-Token des ersten Typs im Tausch gegen Krypto-Token des zweiten Typs implementiert, wobei der Smart Contract eine aktuelle Angebotsgröße, die eine aktuelle Anzahl von Krypto-Token des ersten Typs angibt, und eine Bindungskurve, die eine Funktion definiert, unterhält. Das Erhalten eines Smart Contract ist optional, da die Erzeugungsprozedur und die Vernichtungsprozedur ebenfalls in anderer Software implementiert werden können.
- Die Menge von Krypto-Token des zweiten Typs für den Tausch wird durch Integrieren (520) einer Funktion von der aktuellen Angebotsgröße bis zu einer neuen Angebotsgröße berechnet, wobei die Funktion eine Summe der Bindungskurve und einer Anzahl weiterer Terme ist, wobei die weiteren Terme wenigstens für eine der Erzeugungs- und Vernichtungsprozeduren einen Gebührenterm enthalten, der ein Mehrfaches der um einen Betrag der Krypto-Token des ersten Typs verschobenen Bindungskurve umfasst.

[0168] Fig. 6 zeigt schematisch ein Beispiel einer Ausführungsform eines Verfahrens 600 zum Unterhalten von Krypto-Token eines ersten Typs. Das Verfahren 600 ist computer-implementiert und umfasst Folgendes:

- Erhalten (510) eines Smart Contract von einem verteilten Register, wobei der Smart Contract eine Erzeugungsprozedur zum Erzeugen von Krypto-Token des ersten Typs im Tausch gegen Krypto-Token des zweiten Typs und eine Vernichtungsprozedur zum Vernichten von Krypto-Token des ersten Typs im

Tausch gegen Krypto-Token des zweiten Typs implementiert, wobei der Smart Contract eine aktuelle Angebotsgröße, die eine aktuelle Anzahl von Krypto-Token des ersten Typs angibt, und eine Bindungskurve, die eine Funktion definiert, unterhält,

- wobei das Verfahren in Ansprechen auf das Initiieren (610) der Erzeugungsprozedur Folgendes umfasst:

- Ausführen (620) des Integrierens über eine von der Bindungskurve und von der aktuellen Angebotsgröße abgeleitete Erzeugungsfunktion bis zu dem aktuellen Angebot plus einer Erzeugungsmenge von Krypto-Token des ersten Typs,

- Übertragen (630) der Menge von Krypto-Token des zweiten Typs an einen dem Smart Contract zugeordneten Pool und Übertragen der Menge von Krypto-Token des ersten Typs, und

- Erhöhen (640) der aktuellen Angebotsgröße um die Menge der Krypto-Token des ersten Typs.

- wobei das Verfahren in Ansprechen auf das Initiieren (650) der Vernichtungsprozedur Folgendes umfasst:

- Ausführen (660) des Integrierens über eine von der Bindungskurve und von der aktuellen Angebotsgröße abgeleitete Vernichtungsfunktion bis zu dem aktuellen Angebot minus einer Menge von Krypto-Token des ersten Typs,

- Übertragen (670) der Menge von Krypto-Token des zweiten Typs aus einem dem Smart Contract zugeordneten Pool und Ungültigmachen der Menge von Krypto-Token des ersten Typs, und

- Verringern (680) der aktuellen Angebotsgröße um die Menge der Krypto-Token des ersten Typs und Ungültigmachen der Menge von Krypto-Token des ersten Typs.

[0169] Ferner kann das Verfahren 600 das Übertragen des Zerstörens von Token des ersten Typs, z. B. ihr Ungültigmachen, ihr Übertragen an ein Market-Maker-Wallet usw. umfassen. Die Verfahren 500 und 600 können kombiniert werden, wobei z. B. ein Verfahren zum Unterhalten von Token des ersten Typs sowohl die Erzeugung als auch die Vernichtung der Token umfassen kann.

[0170] Die Verfahren können z. B. computer-implementierte Verfahren sein. Das Erhalten des Smart Contract von einem verteilten Register kann z. B. das Auslesen eines Blocks aus einem verteilten Register, z. B. über ein Computernetz, oder in einer lokalen Datenbank umfassen. Das Ausführen des Smart Contract kann in einem Mikroprozessor erfolgen. Der Smart Contract kann z. B. in einer interpretierenden Sprache geschrieben sein, die durch einen Interpreter, eine virtuelle Maschine oder dergleichen ausgeführt werden kann.

[0171] Das Integrieren einer Kurve kann das Ausführen von Berechnungen, z. B. das Einführen eines aktuellen Angebots und eines neuen Angebots in ein Primitiv oder eine Stammfunktion einer Bindungskurve, eines Integranden in geschlossener Form, umfassen. Das Primitiv kann in geschlossener Form sein und mehrere Primitivsegmente umfassen. Das Empfangen einer Erzeugungs- oder Vernichtungsanforderung kann über ein Computernetz erfolgen. Das Übertragen von Token des ersten Typs oder von Token des zweiten Typs kann ein Schreiben der Übertragung in einen Block zur Aufnahme in einen Block des verteilten Registers umfassen. Der Block kann einen Konsensmechanismus, z. B. einen Proof of Work oder Proof of Stake, umfassen.

[0172] Wie der Fachmann auf dem Gebiet erkennt, sind viele verschiedene Arten der Ausführung der Verfahren möglich. Zum Beispiel kann die Reihenfolge der Schritte in der gezeigten Reihenfolge ausgeführt werden, kann die Reihenfolge der Schritte aber geändert werden oder können einige Schritte parallel ausgeführt werden. Darüber hinaus können zwischen Schritten andere Verfahrensschritte eingefügt werden. Die eingefügten Schritte können Verfeinerungen des Verfahrens wie etwa des hier beschriebenen repräsentieren oder können mit dem Verfahren unzusammenhängend sein. Zum Beispiel können einige Schritte wenigstens teilweise parallel ausgeführt werden. Darüber hinaus kann ein gegebener Schritt nicht vollständig abgeschlossen worden sein, bevor ein nächster Schritt begonnen wird.

[0173] Ausführungsformen des Verfahrens können unter Verwendung von Software ausgeführt werden, die Anweisungen umfasst, um zu veranlassen, dass ein Prozessorsystem das Verfahren 500 und/oder 600 ausführt. Software kann nur jene Schritte enthalten, die durch eine bestimmte Subentität des Systems ergriffen werden. Die Software kann in einem geeigneten Ablagespeichermedium wie etwa einer Festplatte, einer Diskette, einem Speicher, einer optischen Platte usw. gespeichert sein. Die Software kann als ein Signal entlang eines Drahts oder drahtlos oder unter Verwendung eines Datennetzes, z. B. des Internet, gesendet werden.

Die Software kann zum Herunterladen und/oder für die ferne Nutzung in einem Server verfügbar gemacht werden. Ausführungsformen des Verfahrens können unter Verwendung eines Bitstroms ausgeführt werden, der dafür ausgelegt ist, programmierbare Logik, z. B. eine frei programmierbare logische Anordnung (FPGA), zum Ausführen des Verfahrens zu konfigurieren.

[0174] Es wird gewürdigt werden, dass sich der vorliegend offenbarte Gegenstand ebenfalls auf Computerprogramme, insbesondere Computerprogramme auf oder in einem Träger, die dafür ausgelegt sind, den vorliegend offenbarten Gegenstand in die Praxis zu bringen, erstreckt. Das Programm kann in Form von Quellcode, Objektcode, einer Codezwischenquelle und Objektcode wie etwa einer teilweise kompilierten Form oder in irgendeiner anderen Form, die zur Verwendung bei der Implementierung einer Ausführungsform des Verfahrens geeignet ist, sein. Eine Ausführungsform, die sich auf ein Computerprogrammprodukt bezieht, umfasst durch einen Computer ausführbare Anweisungen, die jedem der Verarbeitungsschritte wenigstens eines der dargelegten Verfahren entsprechen. Diese Anweisungen können in Unterprogramme unterteilt sein und/oder in einer oder mehreren Dateien, die statisch oder dynamisch verknüpft sein können, gespeichert sein. Eine andere Ausführungsform, die sich auf ein Computerprogrammprodukt bezieht, umfasst durch einen Computer ausführbare Anweisungen, die jeder der Vorrichtungen, Einheiten und/oder Teile wenigstens eines der dargelegten Systeme und/oder Produkte entsprechen.

[0175] Fig. 7a zeigt ein computer-lesbares Medium 1000 mit einem beschreibbaren Teil 1010 und ein computer-lesbares Medium 1001, ebenfalls mit einem beschreibbaren Teil. Das computer-lesbare Medium 1000 ist in Form eines optisch lesbaren Mediums gezeigt. Das computer-lesbare Medium 1001 ist in Form eines elektronischen Speichers, in diesem Fall einer Speicherkarte, gezeigt. Das computer-lesbare Medium 1000 und 1001 kann Daten 1020 speichern, wobei die Daten Anweisungen angeben können, die, wenn sie durch ein Prozessorsystem ausgeführt werden, veranlassen, dass ein Prozessorsystem eine Ausführungsform eines Verfahrens zum Unterhalten eines Krypto-Tokens gemäß einer Ausführungsform ausführt. Das Computerprogramm 1020 kann in dem computer-lesbaren Medium 1000 als physikalische Marken oder durch Magnetisierung des computer-lesbaren Mediums 1000 verkörpert sein. Allerdings ist irgendeine andere geeignete Ausführungsform ebenfalls denkbar. Obwohl das computer-lesbare Medium 1000 als eine optische Platte gezeigt ist, wird darüber hinaus gewürdigt werden, dass das computer-lesbare Medium 1000 irgendein geeignetes computer-lesbares Medium wie etwa eine Festplatte, ein Festkörperspeicher, ein Flash-Speicher usw. sein kann und nicht beschreibbar oder beschreibbar sein kann. Das Computerprogramm 1020 umfasst Anweisungen, um zu veranlassen, dass ein Prozessorsystem das Verfahren ausführt.

[0176] Fig. 7b zeigt in einer schematischen Darstellung ein Prozessorsystem 1140 gemäß einer Ausführungsform einer Vorrichtung zum Unterhalten eines Krypto-Tokens. Das Prozessorsystem umfasst eine oder mehrere integrierte Schaltungen 1110. Die Architektur der einen oder mehreren integrierten Schaltungen 1110 ist in Fig. 7b schematisch gezeigt. Die Schaltung 1110 umfasst eine Verarbeitungseinheit 1120, z. B. eine CPU, um Computerprogrammkomponenten zum Ausführen eines Verfahrens gemäß einer Ausführungsform und/oder zum Implementieren seiner Module oder Einheiten auszuführen. Die Schaltung 1110 umfasst einen Speicher 1122 zum Speichern von Programmcode, von Daten usw. Ein Teil des Speichers 1122 kann nur lesbar sein. Die Schaltung 1110 kann ein Kommunikationselement 1126, z. B. eine Antenne, Verbinder oder beide und dergleichen, umfassen. Die Schaltung 1110 kann eine dedizierte integrierte Schaltung 1124 zum Ausführen eines Teils oder der gesamten in dem Verfahren definierten Verarbeitung umfassen. Der Prozessor 1120, der Speicher 1122, die dedizierte IC 1124 und das Kommunikationselement 1126 können über eine Verdrahtung 1130, angenommen einen Bus, miteinander verbunden sein. Das Prozessorsystem 1110 kann für die Kontaktkommunikation und/oder kontaktlose Kommunikation unter Verwendung einer Antenne und/oder von Verbindern ausgelegt sein.

[0177] Gemäß einer Ausführungsform kann das Prozessorsystem 1140 z. B. eine Vorrichtung zum Unterhalten eines Krypto-Tokens, eine Prozessorschaltung und eine Speicherschaltung umfassen, wobei der Prozessor dafür ausgelegt ist, in der Speicherschaltung gespeicherte Software auszuführen. Die Prozessorschaltung kann z. B. ein Intel-Core-i7-Prozessor, ein ARM Cortex-R8 usw. sein. Gemäß einer Ausführungsform kann die Prozessorschaltung ein ARM Cortex M0 sein. Die Speicherschaltung kann eine ROM-Schaltung oder ein nichtflüchtiger Speicher, z. B. ein Flash-Speicher, sein. Die Speicherschaltung kann ein flüchtiger Speicher, z. B. ein SRAM-Speicher, sein. In dem letzteren Fall kann die Vorrichtung eine nichtflüchtige Software-Schnittstelle, z. B. ein Festplattenlaufwerk, eine Netzschnittstelle usw. umfassen, die dafür ausgelegt ist, die Software bereitzustellen.

[0178] Es wird angemerkt, dass die oben erwähnten Ausführungsformen den vorliegend offenbarten Gegenstand vielmehr veranschaulichen als beschränken und dass der Fachmann auf dem Gebiet in der Lage ist, viele alternative Ausführungsformen zu entwerfen.

[0179] In den Ansprüchen sind irgendwelche zwischen Klammern angeordneten Bezugszeichen nicht als Beschränkung des Anspruchs zu verstehen. Die Verwendung des Verbs ‚umfassen‘ und seiner Konjugationen schließt die Anwesenheit anderer Elemente oder Schritte als der in einem Anspruch erwähnten nicht aus. Der einem Element vorangehende Artikel ‚ein‘ oder ‚eine‘ schließt die Anwesenheit einer Mehrzahl derartiger Elemente nicht aus. Wenn Ausdrücke wie etwa „wenigstens eines von“ einer Liste von Elementen vorangehen, repräsentieren sie eine Auswahl aller oder irgendeiner Teilmenge von Elementen aus der Liste. Zum Beispiel ist der Ausdruck „wenigstens eines von A, B und C“ so zu verstehen, dass er nur A, nur B, nur C, sowohl A als auch B, sowohl A als auch C, sowohl B als auch C oder alle von A, B und C enthält. Der vorliegend offenbarte Gegenstand kann durch Hardware, die mehrere verschiedene Elemente umfasst, und durch einen geeignet programmierten Computer implementiert werden. In dem Vorrichtungsanspruch, der mehrere Teile aufzählt, können mehrere dieser Teile durch ein und denselben Hardwaregegenstand verkörpert werden. Lediglich die Tatsache, dass bestimmte Maßnahmen in voneinander verschiedenen abhängigen Ansprüchen erwähnt sind, bedeutet nicht, dass eine Kombination dieser Maßnahmen nicht vorteilhaft verwendet werden kann.

[0180] Bezugnahmen in Klammern beziehen sich in den Ansprüchen auf Bezugszeichen in Zeichnungen beispielhafter Ausführungsformen oder auf Formeln von Ausführungsformen, so dass diese die Lesbarkeit des Anspruchs erhöhen. Diese Bezugsnamen sind nicht als Beschränkung des Anspruchs zu verstehen.

ZITATE ENTHALTEN IN DER BESCHREIBUNG

Diese Liste der vom Anmelder aufgeführten Dokumente wurde automatisiert erzeugt und ist ausschließlich zur besseren Information des Lesers aufgenommen. Die Liste ist nicht Bestandteil der deutschen Patent- bzw. Gebrauchsmusteranmeldung. Das DPMA übernimmt keinerlei Haftung für etwaige Fehler oder Auslassungen.

Zitierte Patentliteratur

- WO 2019/043668 A1 [0004]

Patentansprüche

1. Computer-implementiertes Verfahren (500) zum Unterhalten von Krypto-Token eines ersten Typs in einem verteilten Register, wobei das Verfahren Folgendes umfasst:

- Erzeugen von Krypto-Token des ersten Typs im Tausch gegen Krypto-Token des zweiten Typs und Vernichten von Krypto-Token des ersten Typs im Tausch gegen Krypto-Token des zweiten Typs, Unterhalten einer aktuellen Angebotsgröße in dem verteilten Register, die eine aktuelle Anzahl von Krypto-Token des ersten Typs angibt, einer Bindungskurve, die eine Funktion definiert,
- Berechnen der Menge von Krypto-Token des zweiten Typs für den Tausch durch Integrieren (520) einer Funktion von der aktuellen Angebotsgröße bis zu einer neuen Angebotsgröße

$\left(v_{\tau_i^b} = \int_{\tilde{s}}^{\tilde{s}+s_b} \Gamma(x) + \sigma_{p,b} dx + c_{\tau_i^b}; dx + c_{\tau_i^b}; v_{\tau_i^s} = \int_{\tilde{s}-s_s}^{\tilde{s}} \Gamma(x) - \sigma_{p,s} dx - c_{\tau_i^s} \right)$ wobei die Funktion eine Summe der Bindungskurve ($\Gamma(x)$) und einer Anzahl weiterer Terme ist, wobei die weiteren Terme für die Erzeugungs- und/oder Vernichtungsprozedur einen Gebührenterm

$\left(\frac{1}{2} \Gamma(x + s_{fr}) - \frac{1}{2} \Gamma(x); \frac{1}{2} \Gamma(x) - \frac{1}{2} \Gamma(x - s_{fr}); \Gamma(x) - \Gamma(x - s_{fr}) \right)$ enthalten, der ein Mehrfaches der um eine Menge der Krypto-Token des ersten Typs (s_{fr}) verschobenen Bindungskurve umfasst.

2. Verfahren zum Unterhalten von Krypto-Token eines ersten Typs nach Anspruch 1, wobei

- das Verfahren in Ansprechen auf das Initiieren (610) der Erzeugungsprozedur Folgendes umfasst:
- Ausführen (620) des Integrierens über eine von der Bindungskurve und von der aktuellen Angebotsgröße abgeleitete Erzeugungsfunktion bis zu dem aktuellen Angebot plus einer Erzeugungsmenge von Krypto-Token des ersten Typs,
- Übertragen (630) der Menge von Krypto-Token des zweiten Typs an einen Pool und Übertragen der Menge von Krypto-Token des ersten Typs, und
- Erhöhen (640) der aktuellen Angebotsgröße um die Menge von Krypto-Token des ersten Typs.

3. Verfahren zum Unterhalten von Krypto-Token eines ersten Typs nach einem der vorhergehenden Ansprüche, wobei

- das Verfahren in Ansprechen auf das Initiieren (650) der Vernichtungsprozedur Folgendes umfasst:
- Ausführen (660) des Integrierens über eine von der Bindungskurve und von der aktuellen Angebotsgröße abgeleitete Vernichtungsfunktion bis zu dem aktuellen Angebot minus einer Menge von Krypto-Token des ersten Typs,
- Übertragen (670) der Menge von Krypto-Token des zweiten Typs aus einem Pool und Ungültigmachen der Menge von Krypto-Token des ersten Typs, und
- Verringern (680) der aktuellen Angebotsgröße um die Menge von Krypto-Token des ersten Typs und Ungültigmachen der Menge von Krypto-Token des ersten Typs.

4. Verfahren zum Unterhalten von Krypto-Token eines ersten Typs nach einem der vorhergehenden Ansprüche, wobei das Verfahren das Erhalten (510) eines Smart Contract von dem verteilten Register umfasst, wobei das verteilte Register eine Erzeugungsprozedur zum Erzeugen der Krypto-Token des ersten Typs und eine Vernichtungsprozedur für die Vernichtung von Krypto-Token des ersten Typs implementiert, wobei der Smart Contract die aktuelle Angebotsgröße unterhält und die Bindungskurve definiert.

5. Verfahren zum Unterhalten von Krypto-Token eines ersten Typs nach Anspruch 4, wobei der Smart Contract ein Block des verteilten Registers ist.

6. Verfahren zum Unterhalten von Krypto-Token eines ersten Typs nach einem der vorhergehenden Ansprüche, wobei die Bindungskurve durch Parameter, z. B. durch Splines, Geraden, Polynome, Polynom-segmente, definiert ist und wobei die Integration über die Bindungskurve oder über eine von der Bindung abgeleitete Erzeugungsfunktion oder über eine von der Bindungskurve abgeleitete Vernichtungsfunktion durch Anwenden einer Funktion auf die Parameter berechnet wird.

7. Verfahren zum Unterhalten von Krypto-Token eines ersten Typs nach einem der vorhergehenden Ansprüche, wobei

- eine Erzeugungsfunktion von der aktuellen Angebotsgröße bis zu der um eine Erzeugungsmenge erhöhten aktuellen Angebotsgröße integriert wird, wobei die Erzeugungsfunktion die Summe der Bindungskurve und eines Gebührenterms ($\Gamma(x) + \sigma_{p,b}$) ist, und/oder
- eine Vernichtungsfunktion von der aktuellen Angebotsgröße bis zu der um eine Vernichtungsmenge verrin-

gerten aktuellen Angebotsgröße integriert wird; wobei die Vernichtungsfunktion der Rest der Bindungskurve minus einem Gebührenterm ($\Gamma(x) - \sigma_{p,s}$) ist.

8. Verfahren zum Unterhalten von Krypto-Token eines ersten Typs nach einem der vorhergehenden Ansprüche, wobei die Menge der Krypto-Token des zweiten Typs für den Tausch ferner Transaktionskosten $(c_{\tau_i^b})$ für die Erzeugungsprozedur addiert und/oder ferner Transaktionskosten $(-c_{\tau_i^s})$ für die Vernichtungsprozedur subtrahiert.

9. Verfahren zum Unterhalten von Krypto-Token eines ersten Typs nach einem der vorhergehenden Ansprüche, wobei der Gebührenterm proportional zu der Zunahme der Bindungskurve über ein Intervall

$$\left(\left(\frac{1}{2} \Gamma(x + s_{fr}) - \frac{1}{2} \Gamma(x); \frac{1}{2} \Gamma(x) - \frac{1}{2} \Gamma(x - s_{fr}); \Gamma(x) - \Gamma(x - s_{fr}) \right) \right)$$

ist.

10. Verfahren zum Unterhalten von Krypto-Token eines ersten Typs nach einem der vorhergehenden Ansprüche, wobei der Gebührenterm gleich einer ersten Zahl $\left(\frac{1}{2}; 1\right)$ mal einer Differenz der Bindungskurve bei dem aktuellen Angebot und dem aktuellen Angebot plus oder minus einer zweiten Zahl (s_{fr}) ist.

11. Verfahren zum Unterhalten von Krypto-Token eines ersten Typs nach einem der vorhergehenden Ansprüche, wobei

- die Menge der Krypto-Token des ersten Typs, um die die Bindungskurve verschoben wird, konstant ist.

12. Verfahren zum Unterhalten von Krypto-Token eines ersten Typs nach einem der vorhergehenden Ansprüche, wobei das Verfahren Folgendes umfasst:

- Berechnen der Menge von Krypto-Token des ersten Typs, um die die Bindungskurve von dem verteilten Register verschoben wird, insbesondere,
- Berechnen des Volumens der erzeugten und/oder vernichteten Krypto-Token in einer Anzahl jüngster Blöcke in dem verteilten Register, wobei die Menge aus dem Volumen berechnet wird.

13. Verfahren zum Unterhalten von Krypto-Token eines ersten Typs nach einem der vorhergehenden Ansprüche, wobei

- die Erzeugungsprozedur zum Berechnen der Menge von Krypto-Token des zweiten Typs für den Tausch als das Integral $v_{\tau_i^b} = \int_{\tilde{s}}^{\tilde{s}+s_b} \Gamma(x) + \sigma_{p,b} dx + c_{\tau_i^b}$ konfiguriert ist und/oder wobei die Vernichtungsprozedur zum Berechnen der Menge von Token des zweiten Typs für den Tausch als das Integral

$$v_{\tau_i^s} = \int_{\tilde{s}-s_s}^{\tilde{s}} \Gamma(x) + \sigma_{p,s} dx + c_{\tau_i^s} \quad \text{konfiguriert ist, wobei } c_{\tau_i^b} \text{ und } c_{\tau_i^s} \text{ optionale Gebühren sind und wobei}$$

-

$$\sigma^{gfr} = \frac{1}{2} \cdot \begin{cases} \Gamma(x + s_{fr}) - \Gamma(x) & \text{Kauf} \triangleq \sigma_{p,b} \\ \Gamma(x) - \Gamma(x + s_{fr}) & \text{Verkauf} \triangleq \sigma_{p,s} \end{cases}$$

oder

-

$$\sigma^{gfr} = \begin{cases} 0 & \text{Kauf} \triangleq \sigma_{p,b} \\ \Gamma(x) - \Gamma(x + s_{fr}) & \text{Verkauf} \triangleq \sigma_{p,s} \end{cases}$$

ist.

14. Verfahren zum Unterhalten von Krypto-Token eines ersten Typs nach einem der vorhergehenden Ansprüche, wobei eine Erzeugungsfunktion oder eine Vernichtungsfunktion aus einer Bindungskurve als eine Linearkombination eines oder mehrerer der Bindungskurve ($\Gamma(x)$), einer verschobenen Bindungskurve ($\Gamma(x + s_{fr})$; $\Gamma(x - s_{fr})$) und einer optionalen Konstanten abgeleitet wird.

15. Server-Vorrichtung zum Unterhalten von Krypto-Token eines ersten Typs, wobei die Server-Vorrichtung Folgendes umfasst:

- eine Kommunikationsschnittstelle, die konfiguriert ist, Blöcke aus einem verteilten Register zu erhalten,
- ein Prozessorsystem, das konfiguriert ist, eine Erzeugungsprozedur zum Erzeugen von Krypto-Token des ersten Typs im Tausch gegen Krypto-Token des zweiten Typs und eine Vernichtungsprozedur zum Vernichten von Krypto-Token des ersten Typs im Tausch gegen Krypto-Token des zweiten Typs auszuführen, wobei das Prozessorsystem eine aktuelle Angebotsgröße, die eine aktuelle Anzahl von Krypto-Token des ersten Typs angibt und eine Bindungskurve definiert, die eine Funktion definiert, unterhält,
- wobei die Menge von Krypto-Token des zweiten Typs für den Tausch durch Integrieren einer Funktion von der aktuellen Angebotsgröße bis zu einer neuen Angebotsgröße

$\left(v_{\tau_i^b} = \int_{\tilde{s}}^{\tilde{s}+s_b} \Gamma(x) + \sigma_{p,b} dx + c_{\tau_i^b}; dx + c_{\tau_i^b}; v_{\tau_i^s} = \int_{\tilde{s}-s_s}^{\tilde{s}} \Gamma(x) - \sigma_{p,s} dx - c_{\tau_i^s} \right)$ berechnet wird, wobei die Funktion eine Summe der Bindungskurve ($\Gamma(x)$) und einer Anzahl weiterer Terme ist, wobei die weiteren Terme für die Erzeugungs- und/oder Vernichtungsprozedur einen Gebührenterm

$\left(\frac{1}{2} \Gamma(x + s_{fr}) - \frac{1}{2} \Gamma(x); \frac{1}{2} \Gamma(x) - \frac{1}{2} \Gamma(x - s_{fr}); \Gamma(x) - \Gamma(x - s_{fr}) \right)$ enthalten, der ein Mehrfaches der um eine Menge der Krypto-Token des ersten Typs (s_{fr}) verschobenen Bindungskurve umfasst.

16. Client-Vorrichtung zum Unterhalten von Krypto-Token eines ersten Typs, wobei die Client-Vorrichtung Folgendes umfasst:

- eine Kommunikationsschnittstelle, die konfiguriert ist, eine Anforderung zum Erzeugen oder Vernichten einer Menge von Krypto-Token des ersten Typs zu senden, und
- ein Prozessorsystem, das konfiguriert ist zum:
 - Unterhalten eines Wallets mit Krypto-Token des zweiten Typs und zum Übertragen oder Empfangen einer Menge von Krypto-Token des zweiten Typs zu oder von einem Pool,
 - Unterhalten eines Wallets mit Krypto-Token des ersten Typs und zum Übertragen oder Empfangen einer Menge von Krypto-Token des ersten Typs, wobei
 - die Menge von Krypto-Token des zweiten Typs für den Tausch durch Integrieren einer Funktion von der aktuellen Angebotsgröße bis zu einer neuen Angebotsgröße

$\left(v_{\tau_i^b} = \int_{\tilde{s}}^{\tilde{s}+s_b} \Gamma(x) + \sigma_{p,b} dx + c_{\tau_i^b}; dx + c_{\tau_i^b}; v_{\tau_i^s} = \int_{\tilde{s}-s_s}^{\tilde{s}} \Gamma(x) - \sigma_{p,s} dx - c_{\tau_i^s} \right)$ berechnet wird, wobei die Funktion eine Summe der Bindungskurve ($\Gamma(x)$) und einer Anzahl weiterer Terme ist, wobei die weiteren Terme für die Erzeugungs- und/oder Vernichtungsprozedur einen Gebührenterm

$\left(\frac{1}{2} \Gamma(x + s_{fr}) - \frac{1}{2} \Gamma(x); \frac{1}{2} \Gamma(x) - \frac{1}{2} \Gamma(x - s_{fr}); \Gamma(x) - \Gamma(x - s_{fr}) \right)$ enthalten, der ein Mehrfaches der um eine Menge von Krypto-Token des ersten Typs (s_{fr}) verschobenen Bindungskurve umfasst.

17. Transitorisches oder nichttransitorisches computer-lesbares Medium (1000), das Daten (1020) umfasst, die Anweisungen repräsentieren, die, wenn sie durch ein Prozessorsystem ausgeführt werden, veranlassen, dass das Prozessorsystem das Verfahren nach einem der Ansprüche 1-14 ausführt.

Es folgen 8 Seiten Zeichnungen

Anhängende Zeichnungen

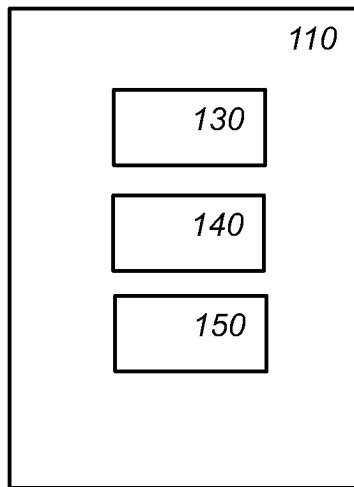


Fig. 1a

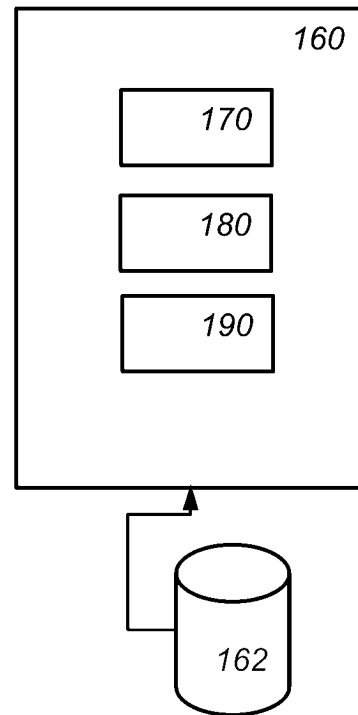


Fig. 1b

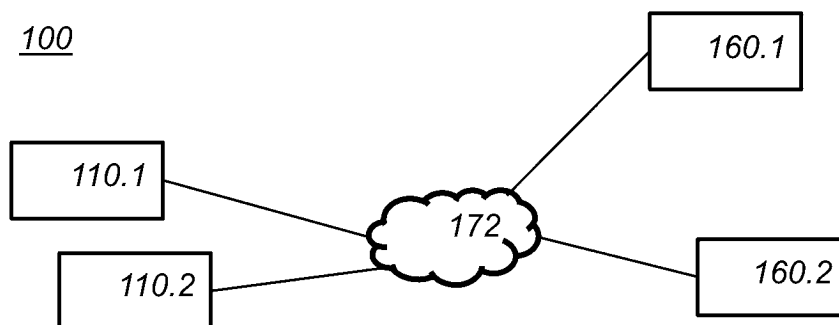


Fig. 1c

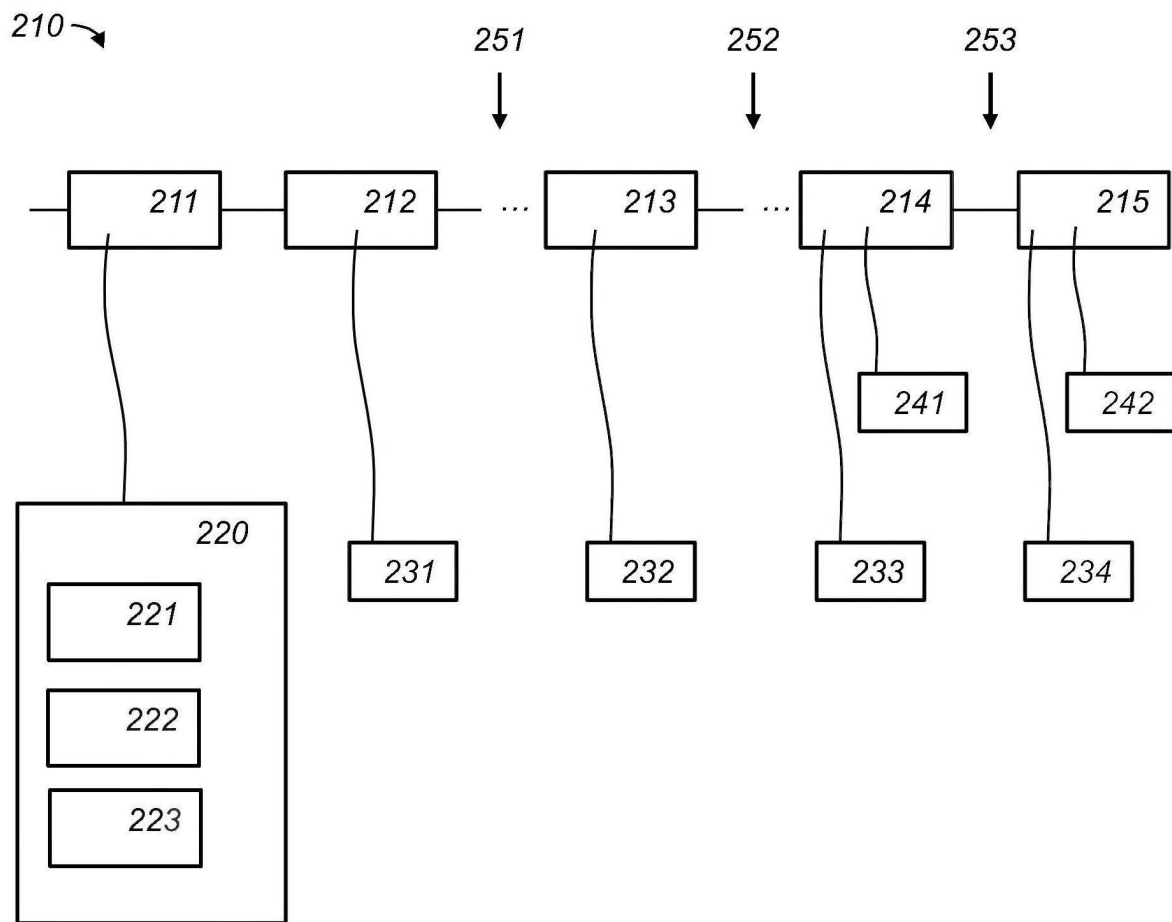


Fig. 2

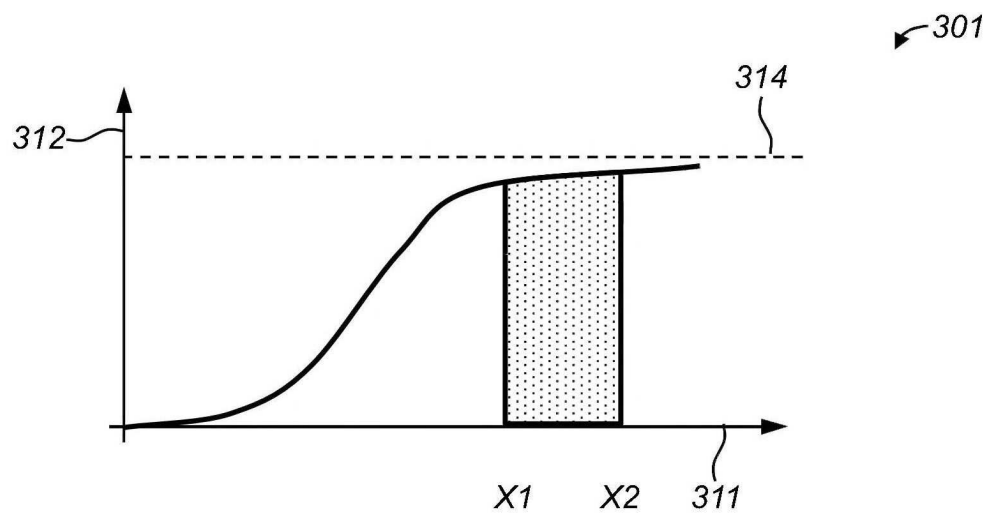


Fig. 3a

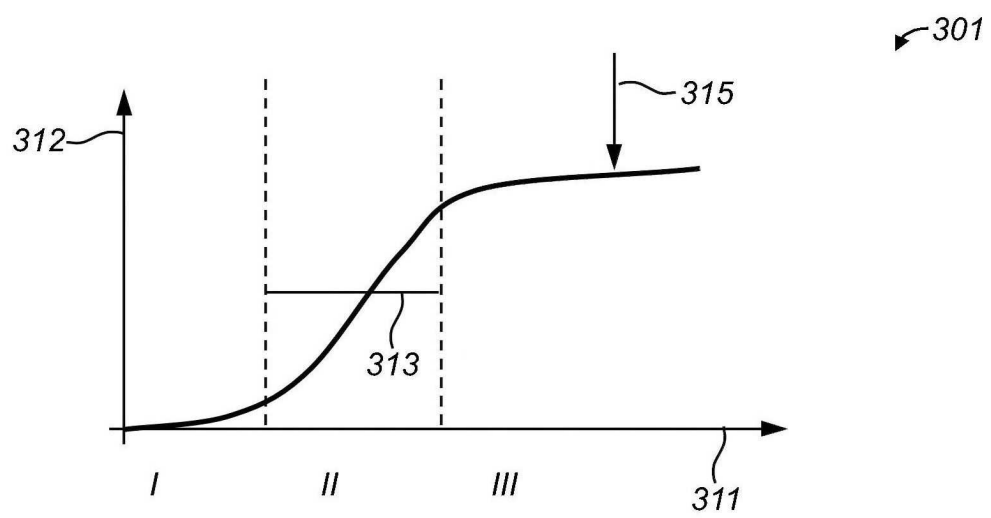


Fig. 3b

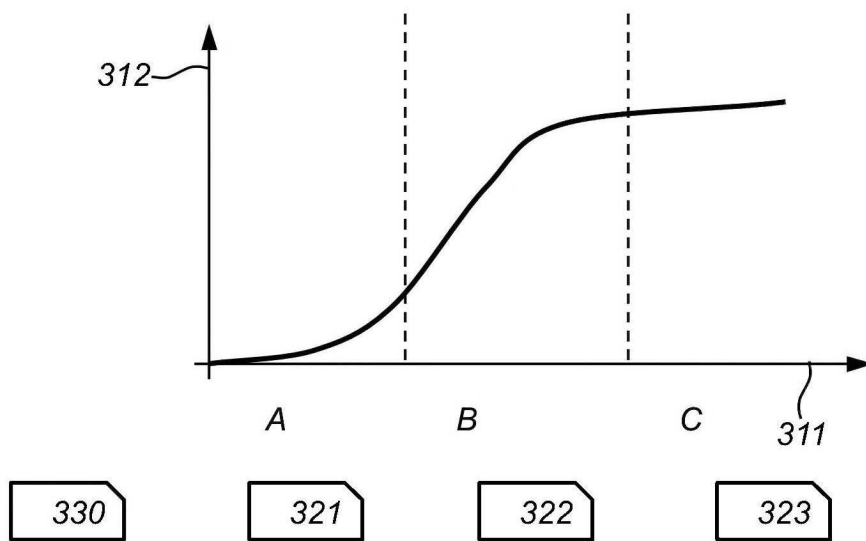


Fig. 3c

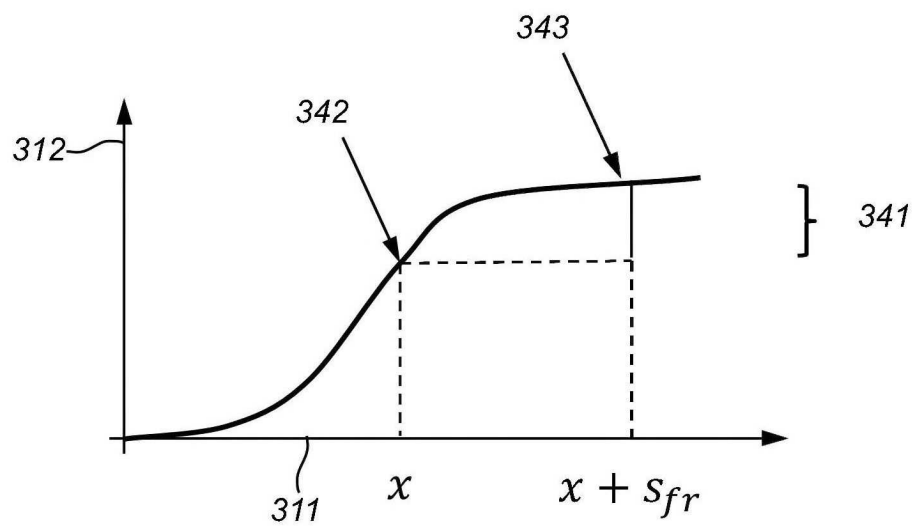


Fig. 3d

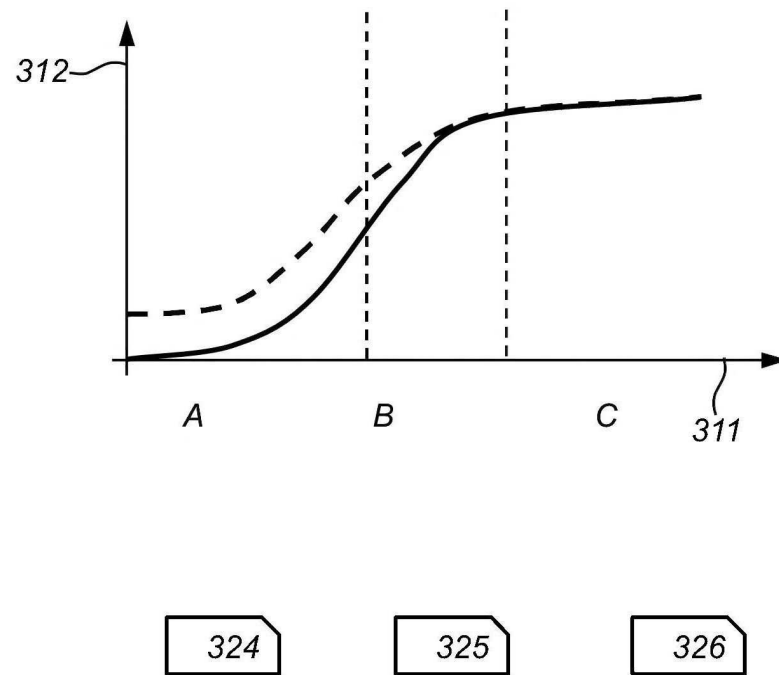


Fig. 4a

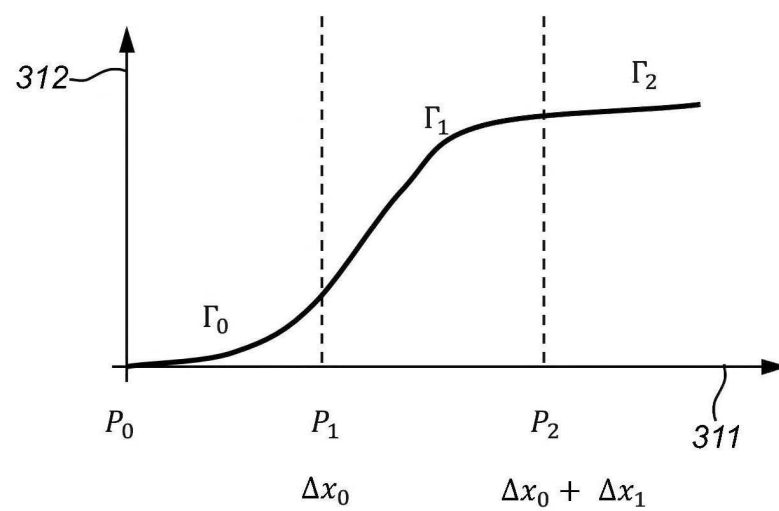


Fig. 4b

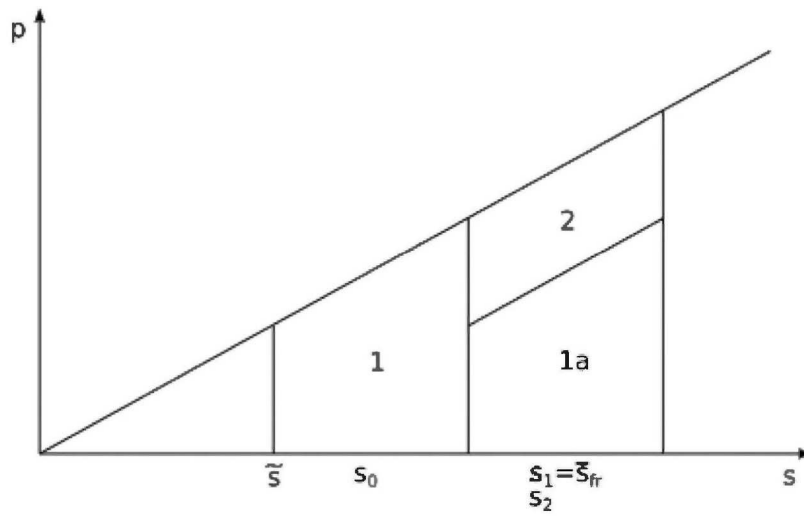


Fig. 4c

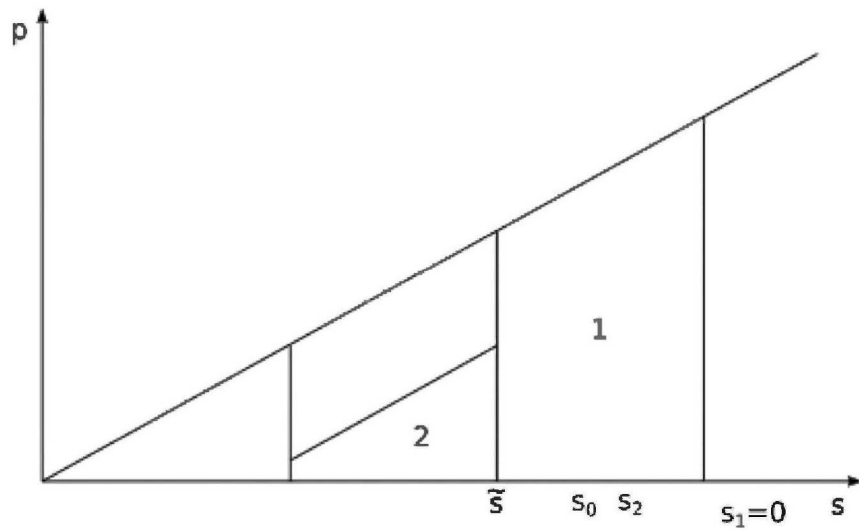
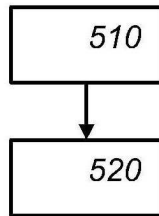


Fig. 4d

500 ↗



600 ↗

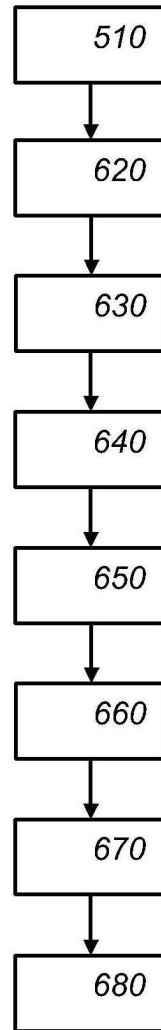


Fig. 5

Fig. 6

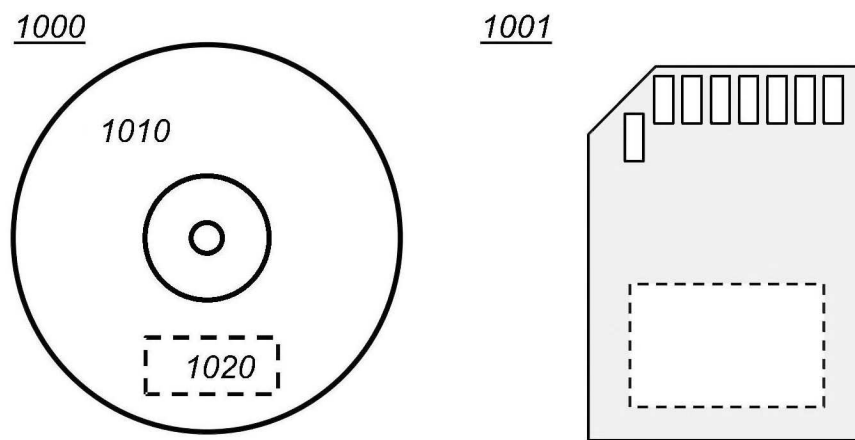


Fig. 7a

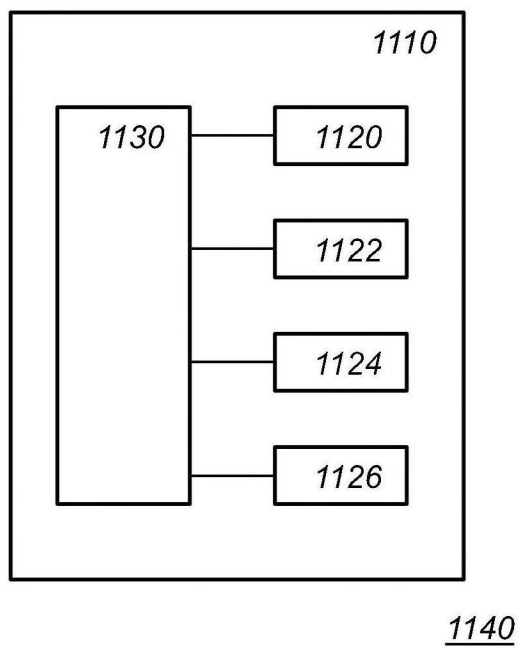


Fig. 7b