

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES
PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro

(43) Internationales Veröffentlichungsdatum
02. September 2021 (02.09.2021)



(10) Internationale Veröffentlichungsnummer
WO 2021/170645 A1

(51) Internationale Patentklassifikation:

G06F 21/64 (2013.01) G06Q 20/36 (2012.01)
G06Q 20/06 (2012.01)

(21) Internationales Aktenzeichen: PCT/EP2021/054543

(22) Internationales Anmeldedatum:
24. Februar 2021 (24.02.2021)

(25) Einreichungssprache: Deutsch

(26) Veröffentlichungssprache: Deutsch

(30) Angaben zur Priorität:
10 2020 104 906.4
25. Februar 2020 (25.02.2020) DE

(71) Anmelder: GIESECKE+DEVRIENT GMBH [DE/DE];
Prinzregentenstraße 159, 81677 München (DE).

(72) Erfinder: FRITZHANNS, Tilo; Rosa-Bavarese-Str. 14,
80639 München (DE). GAWLAS, Florian; Hermann-Vo-
gel-Str. 9, 80805 München (DE). SEIDEMANN, Wolf-
ram; Ottilienstr. 80, 81827 München (DE). VELEVA, Ma-
ria; Konrad-Dreher-Str. 28, 80689 München (DE).

(74) Anwalt: TER MEER STEINMEISTER & PARTNER
PATENTANWÄLTE MBB; Nymphenburger Straße 4,
80335 München (DE).

(81) Bestimmungsstaaten (soweit nicht anders angegeben, für
jede verfügbare nationale Schutzrechtsart): AE, AG, AL,
AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY,
BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM,
DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,
HN, HR, HU, ID, IL, IN, IR, IS, IT, JO, JP, KE, KG, KH,
KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA,
MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI,

(54) Title: METHOD FOR DIRECTLY TRANSMITTING ELECTRONIC COIN DATASETS BETWEEN TERMINALS, PAY-
MENT SYSTEM, PROTECTION SYSTEM, AND MONITORING UNIT

(54) Bezeichnung: VERFAHREN ZUM DIREKTEN ÜBERTRAGEN VON ELEKTRONISCHEN MÜNZDATENSÄTZEN
ZWISCHEN ENDGERÄTEN, BEZAHLSYSTEM, WÄHRUNGSSYSTEM UND ÜBERWACHUNGSEINHEIT

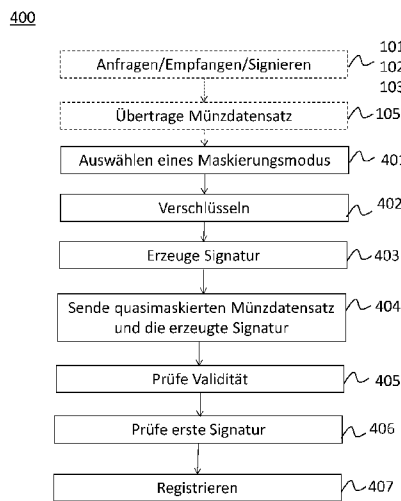


Fig. 13

101, 102, 103 requesting/receiving/signing
105 transmitting coin dataset
401 selecting a masking mode
402 encryption
403 generating signature
404 transmitting semi-masked coin dataset and the generated a signature
405 checking the validity
406 checking first signature
407 registering

(57) Abstract: The invention relates to a method for directly transmitting electronic coin datasets between terminals in order to make a payment in a payment system, wherein a first terminal has at least one electronic coin dataset, and the at least one electronic coin dataset has a monetary value and a concealment value as coin data set elements. The method has the steps of: masking a first coin dataset element of the electronic coin dataset, preferably in the first terminal, by applying a one-way function, which is homomorphic for example, to the first coin dataset element of the electronic coin dataset, preferably to the concealment value thereof, in order to obtain a masked electronic coin dataset element; adding a second coin dataset element of the electronic coin dataset to the semi-masked electronic coin dataset, preferably in the first terminal, in order to obtain a semi-masked electronic coin dataset; and transmitting the semi-masked electronic coin dataset to a monitoring entity in order to register the electronic coin dataset. The invention additionally relates to a payment system with a monitoring layer with a database, in which masked electronic coin datasets are stored, and a direct transaction layer, which uses at least two terminals and in which the method can be carried out.

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren zum direkten Übertragen von elektronischen Münzdatensätzen zwischen Endgeräten zum Bezahlen in einem Bezahlssystem gelöst, wobei ein erstes Endgerät zumindest einen elektronischen Münzdatensatz aufweist, wobei der zumindest eine elektronische Münzdatensatz einen monetären Betrag und einen Verschleierungsbetrag als Münzdatensatzelemente aufweist, mit den Schritten: Maskieren eines ersten Münzdatensatzelements des elektronischen Münzdatensatzes, bevorzugt im ersten Endgerät, durch Anwenden einer Einwegfunktion, die beispielsweise homomorph ist, auf das erste Münzdatensatzelement des elektronischen Münzdatensatzes, bevorzugt auf dessen

NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU,
RW, SA, SC, SD, SE, SG, SK, SL, ST, SV, SY, TH, TJ, TM,
TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM,
ZW.

- (84) Bestimmungsstaaten** (soweit nicht anders angegeben, für jede verfügbare regionale Schutzrechtsart): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), eurasisches (AM, AZ, BY, KG, KZ, RU, TJ, TM), europäisches (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

- mit internationalem Recherchenbericht (Artikel 21 Absatz 3)

Verschleierungsbetrag, zum Erhalten eines maskierten elektronischen Münzdatensatzelements; Hinzufügen eines zweiten Münzdatensatzelements des elektronischen Münzdatensatzes zu dem quasi-maskierten elektronischen Münzdatensatz, bevorzugt im ersten Endgerät, zum Erhalten eines quasi-maskierten elektronischen Münzdatensatzes; und Senden des quasi-maskierten elektronischen Münzdatensatzes an eine Überwachungsinstanz zum Registrieren des elektronischen Münzdatensatzes. Die Erfindung betrifft zudem ein Bezahlungssystem mit einer Überwachungsschicht mit einer Datenbank in der maskierte elektronische Münzdatensätze abgelegt sind; und einer Direkttransaktionsschicht mit zumindest zwei Endgeräten, in welcher das Verfahren durchführbar.

VERFAHREN ZUM DIREKTEN ÜBERTRAGEN VON ELEKTRONISCHEN
MÜNZDATENSÄTZEN ZWISCHEN ENDGERÄTEN, BEZAHLSYSTEM,
WÄHRUNGSSYSTEM UND ÜBERWACHUNGSEINHEIT

5 TECHNISCHES GEBIET DER ERFINDUNG

Die Erfindung betrifft ein Verfahren zum direkten Übertragen von elektronischen Münzdatensätzen zwischen Endgeräten. Weiter betrifft die Erfindung ein Bezahlungssystem zum Austauschen von monetären Beträgen und ein Währungssystem.

10 TECHNISCHER HINTERGRUND DER ERFINDUNG

Sicherheit von Bezahltransaktionen und den dazugehörigen Bezahltransaktionsdaten bedeutet sowohl Schutz der Vertraulichkeit der ausgetauschten Daten; als auch Schutz der Integrität der ausgetauschten Daten; als auch Schutz der Verfügbarkeit der ausgetauschten Daten.

15 Herkömmliche Blockchain-basierte Bezahltransaktionen, wie beispielsweise Bitcoin, stellen einen hohen Schutz der Integrität dar. Wenn elektronische Münzdatensätze, auch „Coins“ genannt, in einer Blockchain-Technologie den Besitzer wechseln, werden viele Informationen veröffentlicht. Somit sind derartige Bezahltransaktionen und insbesondere die ausgetauschten Daten nicht vollkommen vertraulich. Zudem sind die Bezahltransaktionen sehr rechenintensiv und damit
20 energieaufwendig.

Daher werden herkömmlich oft anstelle der vertraulichen Daten nur die Hash-Werte der vertraulichen Daten in einem Blockchain-Ledger abgespeichert. Die korrespondierenden Klartext-Daten müssen dann außerhalb der Blockchain verwaltet werden. Für elektronische
25 Münzdatensätze sind solche Konzepte bislang nicht anwendbar, weil sie grundlegende Kontrollfunktionen, insbesondere (1) das Erkennen von Mehrfachausgabe-Verfahren, auch Double-Spending, genannt und (2) das Erkennen von ungedeckten Zahlungen nicht aufweisen. Im Fall (1) versucht jemand denselben Münzdatensatz mehrfach auszugeben und im zweiten Fall versucht jemand einen Münzdatensatz auszugeben, obwohl er kein Guthaben (mehr) besitzt.

30 Aus der DE 10 2009 038 645 A1 und der DE 10 2009 034 436 A1 sind Systeme zum Übertragen von geldwerten Beträgen in Form elektronischer Datensätze, bei denen ein Bezahlen mit Duplikaten des Datensatzes verhindert und ein hoher Grad an Manipulationssicherheit gegeben ist, bekannt, wobei hier komplexe Strukturen und aufwendige Verschlüsselungs- und
35 Signiervorgänge beim Austausch erforderlich sind. Die haben sich als wenig praxistauglich herausgestellt.

In der WO 2016/200885 A1 ist ein Verfahren zur Verschlüsselung eines in einem Blockchain-Ledger getätigten Betrags beschrieben, wobei die Verifizierbarkeit der Transaktion erhalten bleibt.

Dabei wird ein Verschleierungsbetrag zu einem Eingangswert addiert. Dann wird ein Ausgangswert erzeugt und verschlüsselt. Sowohl der Eingangswert als auch der Ausgangswert liegen innerhalb eines Wertebereichs, wobei eine Summe von zwei beliebigen Werten innerhalb des Bereichs einen Schwellenwert nicht überschreitet. Die Summe aus dem verschlüsselten Eingangswert und dem verschlüsselten Ausgangswert kann gleich Null sein. Bereichsprüfungen, sogenannte Range-Proofs, sind jedem der Eingangswerte und dem Ausgangswert zugeordnet. Diese Bereichsprüfungen beweisen, dass der Eingangswert und der Ausgangswert in den Wertebereich fallen. Jeder öffentliche Schlüssel kann mit einer Ringsignatur signiert werden, die auf einem öffentlichen Schlüssel eines Empfängers in der Transaktion basiert. In diesem Verfahren ist eine Blockchain-Technologie notwendig, die nach Erhalt eines Münzdatensatzes angerufen werden muss, um den Münzdatensatz zu validieren.

Es ist Aufgabe der vorliegenden Erfindung, ein Verfahren und ein System zu schaffen, in denen eine Bezahltransaktion sicher aber dennoch einfach ausgestaltet ist. Dabei soll insbesondere eine direkte Bezahlung zwischen Geräten, wie Token, Smartphones aber auch Maschinen, wie Kassenterminals oder Automaten, geschaffen werden, die anonym ist. Die Münzdatensätze sollen nach dem Erhalt sofort weiterverwendet werden können, um eine Bezahlung auch ohne Verbindung zu einer Online-Einheit, beispielsweise einer DLT, zu ermöglichen. Mehrere Münzdatensätze sollen beim Benutzer beliebig miteinander kombiniert und/oder aufgeteilt werden können, um ein flexibles Austauschen zu ermöglichen. Die ausgetauschten Münzdatensätze sollen einerseits vertraulich gegenüber anderen Systemteilnehmern sein, aber andererseits jedem Systemteilnehmer erlauben, grundlegende Überwachungsprüfungen durchzuführen, insbesondere das Erkennen von Mehrfach-Ausgabe-Versuchen und das Erkennen von Versuchen mit nicht vorhandenen Beträgen zu zahlen. Es soll perspektivisch möglich sein, ganz auf Bargeld (Banknoten und analoge Münzen), zumindest aber auf analoge Münzen, zu verzichten.

Das Modifizieren, also beispielsweise das Aufteilen, das Verbinden (=Kombinieren) oder das Umschalten der elektronischen Münzdatensätze soll ohne hohen Rechenaufwand und mit minimalem Datenvolumen für die Übertragung der Münzdatensätze erfolgen. Das Verifizieren des Modifizierens soll ohne aufwendiges Nachweisen entsprechender Gültigkeit (Range-Proofs) sicher erfolgen können, um den Grad an Flexibilität und damit die Nutzerfreundlichkeit zu erhöhen.

ZUSAMMENFASSUNG DER ERFINDUNG

Die gestellten Aufgaben werden mit den Merkmalen der unabhängigen Patentansprüche gelöst. Weitere vorteilhafte Ausgestaltungen sind in den abhängigen Patentansprüchen beschrieben.

Die Aufgabe wird insbesondere durch ein Verfahren zum direkten Übertragen von elektronischen Münzdatensätzen zwischen Endgeräten zum Bezahlen in einem Bezahlssystem gelöst, wobei ein

erstes Endgerät zumindest einen elektronischen Münzdatensatz aufweist, wobei der zumindest eine elektronische Münzdatensatz einen monetären Betrag und einen Verschleierungsbetrag als Münzdatensatzelemente aufweist, mit den Schritten: Maskieren eines ersten Münzdatensatzelements des elektronischen Münzdatensatzes, bevorzugt im ersten Endgerät, durch Anwenden einer Einwegfunktion, die beispielsweise homomorph ist, auf das erste Münzdatensatzelement des elektronischen Münzdatensatzes, bevorzugt auf dessen Verschleierungsbetrag, zum Erhalten eines maskierten ersten elektronischen Münzdatensatzelements; Hinzufügen eines zweiten Münzdatensatzelements des elektronischen Münzdatensatzes zu dem maskierten ersten elektronischen Münzdatensatzelement, bevorzugt im ersten Endgerät, zum Erhalten eines quasi-maskierten elektronischen Münzdatensatzes; und Senden des quasi-maskierten elektronischen Münzdatensatzes an eine Überwachungsinstanz zum Registrieren des elektronischen Münzdatensatzes.

Somit wird in einem Zwischenergebnis ein maskiertes Münzdatensatzelement errechnet (erhalten) und dieses dann mit einem Münzdatensatzelement des Münzdatensatzes erweitert.

Das hinzuzufügende Münzdatensatzelement ist unmaskiert. Es kann in einer Ausgestaltung des Verfahrens direkt aus dem entsprechenden Münzdatensatz entnommen werden. Es wird dem vollständig maskierten Münzdatensatz hinzugefügt und kann ohne Demaskieren des Münzdatensatzes ausgelesen, entnommen und/oder interpretiert werden.

Das erste Münzdatensatzelement des Maskieren-Schritts ist vom zweiten Münzdatensatzelement des Hinzufügen-Schritts verschieden.

Mit diesem Verfahren wird sichergestellt, dass der elektronische Münzdatensatz nicht offengelegt an die Überwachungsinstanz gesendet wird, aber dennoch eine Überprüfung in der Überwachungsinstanz hinreichend sicher durchgeführt werden kann.

Das Hinzufügen wird durch eine entsprechende (logische) Operation durchgeführt. Diese Operation fügt das maskierte erste elektronische Münzdatensatzelement und das zweite Münzdatensatzelement des Münzdatensatzes zusammen. Es entsteht dadurch ein neuer Datensatz, nämlich der quasi-maskierte elektronische Münzdatensatz. Das Hinzufügen wird beispielsweise auch als Konkatenation oder Verkettung oder Anfügen bezeichnet. Auch eine Datenstruktur, wie TLV, kann vorgesehen sein, um das maskierte erste elektronische Münzdatensatzelement und das zweite Münzdatensatzelement des Münzdatensatzes zum quasi-maskierten elektronischen Münzdatensatz zusammenzuführen.

In einer bevorzugten Ausgestaltung ist das erste Münzdatensatzelement des Maskieren-Schritts der Verschleierungsbetrag des elektronischen Münzdatensatzes. Der Verschleierungsbetrag stellt

ein Geheimnis für die Überwachungsinstanz dar und ist nur in einer Direkttransaktionsschicht zwischen denjenigen Teilnehmern bekannt, die sich den Münzdatensatz gegenseitig übertragen.

5 In einer bevorzugten Ausgestaltung ist das hinzugefügte (zweite) Münzdatensatzelement der monetäre Betrag des elektronischen Münzdatensatzes. Dadurch wird ein betragsteiloffener maskierter elektronischer Münzdatensatz als der quasi-maskierte elektronische Münzdatensatz erhalten. Mit einem derartigen quasi-maskierte elektronischen Münzdatensatz kann der monetäre Betrag sofort und ohne weitere Entschlüsselungs- oder Demaskieren-Schritte ausgelesen und interpretiert werden. Damit werden Teile des quasi-maskierten elektronischen Münzdatensatzes
10 offen (betragsteiloffen) übertragen und registriert, andere Teile werden maskiert übertragen und registriert. Damit bleibt das Verfahren anonym und sicher, die übertragenen geldwerten Beträge können aber jederzeit verfolgt und registriert werden. Der Bezahlvorgang ist damit weiterhin anonym, obwohl die Betragstransfers transparent sind.

15 In einer bevorzugten Ausgestaltung ist das hinzugefügte (zweite) Münzdatensatzelement ein höherwertiger Betragsanteil des stellenweise in den höherwertigen und einen niederwertigen Betragsanteil aufgeteilten monetären Betrages des elektronischen Münzdatensatzes, wodurch ein nur hinsichtlich des höherwertigen Betragsanteils betragsteiloffener elektronischer Münzdatensatz als der quasi-maskierte elektronische Münzdatensatz erhalten wird. Mit einem derartigen
20 elektronischen Münzdatensatz kann der höherwertige Betragsanteil sofort und ohne weitere Entschlüsselungs- oder Demaskieren-Schritte ausgelesen und interpretiert werden. Damit bleibt das Verfahren anonym und es ist zudem nicht offen verfügbar, welche Geldbeträge zwischen den Teilnehmereinheiten übertragen wird, die übertragenen geldwerten Beträge können dem Grunde nach jederzeit verfolgt und registriert werden. Der Bezahlvorgang ist damit weiterhin anonym,
25 obwohl die Betragstransfers semi-transparent sind.

Bevorzugt ist der quasi-maskierte elektronische Münzdatensatz dann nur hinsichtlich des niederwertigen Betragsanteils maskiert.

30 Der höherwertige Betragsanteil repräsentiert einen Anteil des monetären Betrags der größer ist als der Anteil des monetären Betrags, der den niederwertigen Betragsanteil repräsentiert. Beispielsweise können höherwertige Stellen eines den monetären Betrag repräsentierenden (zweiten) Münzdatensatzelements, beispielsweise ein oder mehrere „most-significant bits, MSB“, transparent übertragen werden. Übrige, niederwertige Stellen des, den monetären Betrag
35 repräsentierenden Datenelements werden maskiert.

In einer bevorzugten Ausgestaltung umfasst das Verfahren weiter: Festlegen eines Maskierungsmodus aus zumindest zwei Maskierungsmodi, wobei in einem ersten Maskierungsmodus der quasi-maskierte elektronische Münzdatensatz an die

Überwachungsinstanz zum Zweck des Registrierens gesendet wird und wobei in einem zweiten Maskierungsmodus der elektronische Münzdatensatz, bevorzugt im ersten Endgerät, durch Anwenden einer Einwegfunktion, die beispielsweise homomorph ist, auf den elektronischen Münzdatensatz zum Erhalten eines vollständig maskierten elektronischen Münzdatensatzes maskiert wird und der vollständig maskierte elektronische Münzdatensatz an die Überwachungsinstanz zum Zweck des Registrierens gesendet wird. Damit wird eine Maskierungsart auswählbar und konfigurierbar. Im Bezahlungssystem kann damit pro Übertragungsvorgang und/oder generell festgelegt werden, mit welchem Grad an Anonymität die Münzdatensätze registriert werden sollen.

Bei Verwendung des zweiten Maskierungsmodus wird auf den Hinzufügen-Schritt verzichtet und es ist kein unmaskiertes Münzdatensatzelement im maskierten Münzdatensatz enthalten oder angefügt.

In einer bevorzugten Ausgestaltung umfasst das Verfahren einen dritten Maskierungsmodus mit: stellenwertweises Aufteilen des monetären Betrags des elektronischen Münzdatensatzes, bevorzugt im ersten Endgerät, in einen ersten monetären Betragsteil und in einen zweiten monetären Betragsteil, wobei die Basis des Stellenwerts beliebig ist: Maskieren des ersten monetären Betragsteils des monetären Betrags des elektronischen Münzdatensatzes, bevorzugt im ersten Endgerät, durch Anwenden der Einwegfunktion auf den ersten monetären Betragsteil des monetären Betrags des elektronischen Münzdatensatzes zum Erhalten eines maskierten ersten monetären Betragsteils und Hinzufügen (nur) des zweiten monetären Betragsteils zum Erhalten eines teilbetragsmaskierten (nachfolgend auch als teilmaskiert bezeichnet) elektronischen Münzdatensatzes. Die Auswahl des Stellenwerts erfolgt entweder anhand eines verfahrenswelt vorgegebenen Vorgabewertes oder zufallsbasiert oder entsprechend einer Wahl des Endgeräts.

In einer Ausgestaltung des dritten Maskierungsmodus wird die Einwegfunktion auf eine Verknüpfung (Verkettung) von Verschleierungsbetrag und ersten monetären Betragsteils des elektronischen Münzdatensatzes angewendet, um eine maskierte Verknüpfung aus Verschleierungsbetrag und erstem monetären Betragsteil (als maskierten ersten Münzdatensatz) zu erhalten. Dieser maskierten Verknüpfung wird der zweite Betragsteil hinzugefügt, um den teilbetragsmaskierten elektronischen Münzdatensatz zu erhalten.

In einer bevorzugten Ausgestaltung ist der Schritt des Registrierens in Abhängigkeit des festgelegten Maskierungsmodus entweder das Registrieren des vollständig maskierten elektronischen Münzdatensatzes (für den zweiten Maskierungsmodus) oder des quasi-maskierten elektronischen Münzdatensatzes (für den ersten Maskierungsmodus) des teilbetragsmaskierten elektronischen Münzdatensatzes in der Überwachungsinstanz (für den dritten Maskierungsmodus).

Das Festlegen beziehungsweise das Auswählen des Maskierungsmodus kann im Verfahren fest vorgegeben sein, beispielsweise durch die Überwachungsinstanz oder einen Drittanbieter (Wallet-Anbieter). Damit wäre ein Verfahren vorgesehen, in welchem der Maskierungsmodus fest vorgegeben ist.

Alternativ könnte der Schritt des Festlegens durch ein Auswählen des Maskierungsmodus im ersten Endgerät erfolgen. Damit wäre ein agiles Verfahren vorgesehen, in welchem das jeweilige Endgerät den Maskierungsmodus selbst festlegt bzw. auswählt oder einem Benutzer des Endgeräts eine Möglichkeit zur Auswahl bereitstellt. Das Festlegen des Maskierungsmodus wäre dann beispielsweise pro Übertragungsvorgang möglich, sodass sich das Übertragen beispielsweise daran orientiert, ob der Empfänger des Münzdatensatzes im Bezahlungssystem bekannt und validiert ist oder nicht.

In einer bevorzugten Ausgestaltung wird ein Parameter zum Festlegen des Maskierungsmodus von der Überwachungsinstanz oder einem Diensteanbieter vorgegeben. Bevorzugt wählt dann das Endgerät den Maskierungsmodus anhand dieses Parameters aus. Somit ist ein Endgerät eingerichtet, anhand des Parameters situationsbedingt zu entscheiden welcher Maskierungsmodus ausgewählt beziehungsweise festgelegt wird. Ein Parameter zum Vorgeben des Maskierungsmodus könnte beispielsweise eine Mindestrechenleistung des Endgeräts oder eine maximale Zeitdauer zum Maskieren und Registrieren des Münzdatensatzes oder ein Grad an Geheimhaltung für den Münzdatensatz sein. Insbesondere kann dadurch ein vom ersten Endgerät verschiedenes anderes Endgerät möglicherweise einen anderen Maskierungsmodus auswählen, um den Vorgabeparameter einzuhalten.

In einer bevorzugten Ausgestaltung wird von einem (zuerst verwendeten) Maskierungsmodus in einen (darauffolgenden) anderen Maskierungsmodus für einen elektronischen Münzdatensatz durch das Endgerät gewechselt. Damit wird eine Interoperabilität zwischen einem vollständig maskierten, einem quasimaskierten und einem teilbetragsmaskierten elektronischen Münzdatensatz geschaffen, wodurch die Flexibilität des Übertragens vergrößert wird.

Beispielsweise kann ein quasi-maskierter Münzdatensatz mit einem vollständig maskierten elektronischen Münzdatensatz verbunden werden. Dazu könnte man den vollständig maskierten Münzdatensatz in einen quasi-maskierten Münzdatensatz umschalten („switch“) oder umgekehrt.

Die hier beschriebenen Schritte müssen nicht in der beschriebenen Reihenfolge durchgeführt werden. Die hier beschriebene Reihenfolge ist jedoch eine bevorzugte Ausgestaltung.

Ein elektronischer Münzdatensatz ist ein elektronischer Datensatz, der durch Münzdatensatzelemente repräsentiert ist. Er ist insbesondere ein elektronischer Datensatz, der einen geldwerten (=monetären) Betrag repräsentiert und umgangssprachlich auch als „digitale Münze“ oder „elektronische Münze“, englisch „digital/electronic coin“ bezeichnet wird. Dieser geldwerte Betrag wechselt bei dem Verfahren von einem ersten Endgerät zu einem anderen Endgerät zum Bezahlen (eines Kaufpreises oder eines Rückgeldes) im Bezahlssystem. Als ein geldwerter Betrag als Münzdatensatzelement wird im Folgenden ein digitaler Betrag verstanden, der z.B. auf einem Konto eines Geldinstituts gutgeschrieben werden kann, oder gegen ein anderes Zahlungsmittel getauscht werden kann. Ein elektronischer Münzdatensatz repräsentiert also Bargeld in elektronischer Form.

Das Endgerät kann eine Vielzahl von elektronischen Münzdatensätzen aufweisen, beispielsweise kann in einem Datenspeicher des Endgeräts die Vielzahl von Münzdatensätzen hinterlegt sein. Der Datenspeicher stellt dann beispielsweise eine elektronische Geldbörse dar. Der Datenspeicher kann beispielsweise intern, extern oder virtuell sein. In einer Ausgestaltung kann beim Empfangen eines elektronischen Münzdatensatzes automatisch ein „Verbinden“ stattfinden, sodass bevorzugt nur ein (oder eine bestimmte Anzahl an) elektronischer(n) Münzdatensatz/sätzen im Endgerät abgelegt sind.

Das Endgerät kann beispielsweise ein passives Gerät, wie z. B. ein Token, ein mobiles Endgerät, wie z.B. ein Smartphone, ein Tablet-Computer, ein Computer, ein Server oder eine Maschine sein.

Ein elektronischer Münzdatensatz zum Übertragen von geldwerten Beträgen unterscheidet sich wesentlich von einem elektronischen Datensatz zum Datenaustausch oder Datentransfer, da beispielsweise eine klassische Datentransaktion auf Basis eines Frage-Antwort-Prinzips bzw. auf einer Interkommunikation zwischen den Datentransferpartnern stattfindet. Ein elektronischer Münzdatensatz ist dementsgegen einmalig, eindeutig und steht im Kontext eines Sicherheitskonzepts, welches beispielsweise Signaturen oder Verschlüsselungen umfassen kann. In einem elektronischen Münzdatensatz sind prinzipiell alle Daten enthalten, die für eine empfangende Instanz bezüglich Verifikation, Authentisierung und Weitergeben an andere Instanzen benötigt werden. Eine Interkommunikation zwischen den Endgeräten beim Austausch ist daher bei dieser Art Datensätze grundsätzlich nicht erforderlich.

Bevorzugt wird der elektronische Münzdatensatz vom ersten Endgerät an ein zweites Endgerät im Rahmen eines Bezahlvorgangs übertragen.

Erfindungsgemäß weist ein zum Übertragen zwischen zwei Endgeräten verwendeter elektronischer Münzdatensatz einen monetären Betrag als ein Münzdatensatzelement, das einen Geldwert des elektronischen Münzdatensatzes darstellt, und einen Verschleierungsbetrag, als

Münzdatensatzelement, beispielsweise eine Zufallszahl, auf. Darüber hinaus kann der elektronische Münzdatensatz weitere Münzdatensatzelemente, wie Metadaten, aufweisen, welche beispielsweise eine Währung des monetären Betrags oder eine Kennung des Münzdatensatzes repräsentiert. Ein elektronischer Münzdatensatz wird durch diese wenigstens beiden
5 Münzdatensatzelemente (monetärer Betrag und Verschleierungsbetrag) eindeutig repräsentiert. Jeder, der Zugriff auf diese zumindest zwei Münzdatensatzelemente eines gültigen elektronischen Münzdatensatzes hat, kann diesen elektronischen Münzdatensatz zum Bezahlen verwenden. Die Kenntnis dieser beiden Münzdatensatzelemente (monetärer Betrag und Verschleierungsbetrag) ist also gleichbedeutend mit dem Besitz des digitalen Geldes. Dieser elektronische Münzdatensatz
10 wird zwischen zwei Endgeräten direkt übertragen. In einer Ausgestaltung der Erfindung besteht ein elektronischer Münzdatensatz aus diesen beiden Münzdatensatzelementen, es ist somit zum Austausch von digitalem Geld nur die Übertragung des monetären Betrags und der Verschleierungsbetrag notwendig.

15 Zu jedem elektronischen Münzdatensatz wird ein entsprechender maskierter elektronischer Münzdatensatz und/oder ein maskiertes erstes Münzdatensatzelement zugeordnet. Dieser maskierte elektronischer Münzdatensatz kann ein vollständig maskierter elektronischer Münzdatensatz (zweiter Maskierungsmodus) oder ein quasi-maskierter elektronischer Münzdatensatz (erster Maskierungsmodus) oder ein teilbetragsmaskierter elektronischer
20 Münzdatensatz (dritter Maskierungsmodus) sein.

Ein vollständig maskierter elektronischer Münzdatensatz (zweiter Maskierungsmodus) ist ein maskierter elektronischer Münzdatensatz, dessen Gesamtheit von Münzdatensatzelementen maskiert ist. Der vollständig maskierte elektronische Münzdatensatz umfasst insbesondere kein
25 unmaskiertes Datensatzelement. Aus dem vollständig maskierten elektronischen Münzdatensatz kann kein (unmaskiertes) Datensatzelement des elektronischen Münzdatensatz direkt entnommen, abgelesen und/oder interpretiert werden.

Ein quasimaskierter elektronischer Münzdatensatz (zweiter Maskierungsmodus) ist ein maskierter
30 elektronischer Münzdatensatz, bei dem zumindest ein (erstes) Münzdatensatzelement des (nicht maskierten) elektronischen Münzdatensatzes in kryptografischer verschlüsselter Form enthalten ist. Der quasi-maskierte elektronische Münzdatensatz wird durch Anwenden einer Einwegfunktion, beispielsweise einer kryptografischen Verschlüsselungsfunktion, auf zumindest eines der Münzdatensatzelemente, bevorzugt den Verschleierungsbetrag, und Hinzufügen eines
35 unmaskierten zweiten Münzdatensatzelements erhalten. Der quasimaskierte elektronische Münzdatensatz umfasst also neben dem verschlüsselten ersten Münzdatensatzelement insbesondere auch zumindest ein zweites unmaskiertes Münzdatensatzelement, insbesondere den monetären Betrag als zweites Münzdatensatzelement. Aus dem quasimaskierten elektronischen Münzdatensatz kann zumindest ein (unmaskiertes) Münzdatensatzelement des elektronischen

Münzdatensatz direkt entnommen werden. Das unmaskierte Münzdatensatzelement kann dem maskierten Münzdatensatzelement hinzugefügt werden, um den quasi-maskierten Münzdatensatz zu erhalten.

- 5 Ein teilbetragsmaskierter elektronischer Münzdatensatz (dritter Maskierungsmodus) ist ein maskierter elektronischer Münzdatensatz, bei dem zumindest ein erster monetäre Betragsteil des monetären Betrags des elektronischen Münzdatensatz in maskierter, beispielsweise kryptografisch verschlüsselter, Form enthalten ist und ein zweiter Betragsteil des monetären Betrags des elektronischen Münzdatensatzes offen (unmaskiert) enthalten ist. Der teilbetragsmaskierte elektronische Münzdatensatz umfasst daher auch ein unmaskiertes Münzdatensatzteilelement, insbesondere den zweiten monetären Betragsteil. Der erste monetäre Betragsteil und der zweite monetäre Betragsteil wurden durch stellenwertweises Aufteilen des monetären Betrags des elektronischen Münzdatensatzes erhalten, siehe unten angegebene weiterführende Erläuterungen zum Stellenwert und der Basis. Der zweite monetäre Betragsteil wird unmaskiert zum maskierten ersten monetären Betragsteil des monetären Betrags hinzugefügt. Aus dem teilbetragsmaskierten elektronischen Münzdatensatz kann demnach zumindest der zweite monetäre Betragsteil des elektronischen Münzdatensatz direkt entnommen werden.

Beim teilbetragsmaskierten elektronischen Münzdatensatz wird bevorzugt das Festlegen des Stellenwerts zum Aufteilen des monetären Betrags in den ersten Betragsteil und den zweiten Betragsteil transaktionsabhängig variabel. Damit ist die Überprüfung eines empfangenen Münzdatensatzes abhängig von der Kenntnis über den festgelegten Stellenwert. Dieser festgelegte Stellenwert wird entweder bei der Transaktion zwischen den Endgeräten bzw. Teilnehmereinheiten mit übertragen oder im Register mit abgelegt.

25 Nachfolgend wird zur Vereinfachung immer der Begriff „maskierter elektronischer Münzdatensatz“ verwendet, wenn eine Aussage sowohl für einen vollständig maskierten elektronischen Münzdatensatz als auch einen für einen quasimaskierten elektronischen Münzdatensatz als auch einen teilbetragsmaskierten elektronischen Münzdatensatz gleichermaßen zutrifft.

Die Kenntnis eines maskierten elektronischen Münzdatensatzes berechtigt nicht dazu, das digitale Geld, das durch den elektronischen Münzdatensatz repräsentiert wird, auszugeben. Dies stellt einen wesentlichen Unterschied zwischen den maskierten elektronischen Münzdatensätze und den (nicht maskierten) elektronischen Münzdatensätzen dar und ist ein Kern der hier vorliegenden Erfindung. Der maskierte elektronische Münzdatensatz ist einzigartig und eindeutig einem elektronischen Münzdatensatz zuzuordnen, es herrscht also eine 1-zu-1 Beziehung zwischen dem (nicht-maskierten) elektronischen Münzdatensatz und dem maskierten elektronischen Münzdatensatz. Das Maskieren des elektronischen Münzdatensatzes erfolgt bevorzugt durch eine

Recheneinheit des Endgeräts innerhalb des Endgeräts, das auch den zumindest einen elektronische Münzdatensatz aufweist. Alternativ kann das Maskieren durch eine Recheneinheit des Endgeräts, das den elektronischen Münzdatensatz empfängt, erfolgen.

5 Der maskierte elektronische Münzdatensatz wird durch Anwenden einer Einwegfunktion, beispielsweise einer homomorphen Einwegfunktion, beispielsweise einer kryptographischen Funktion, erhalten. Diese Funktion ist eine Einwegfunktion, also eine mathematische Funktion, die komplexitätstheoretisch „leicht“ berechenbar, aber „schwer“ bis praktisch unmöglich umzukehren ist. Hierbei wird unter Einwegfunktion auch eine Funktion bezeichnet, zu der bislang
10 keine in angemessener Zeit und mit vertretbarem Aufwand praktisch ausführbare Umkehrung bekannt ist. Somit ist die Berechnung eines maskierten elektronischen Münzdatensatzes aus einem elektronischen Münzdatensatz vergleichbar mit bzw. entspricht der Generierung eines öffentlichen Schlüssels in einem Verschlüsselungsverfahren über eine Restklassengruppe. Vorzugsweise wird eine Einwegfunktion verwendet, die auf eine Gruppe operiert, in der das diskrete
15 Logarithmusproblem schwer zu lösen ist, wie z. B. ein kryptographisches Verfahren analog einer elliptischer-Kurve-Verschlüsselung, kurz ECC, aus einem privaten Schlüssel eines entsprechenden Kryptographie-Verfahrens. Die umgekehrte Funktion, also die Erzeugung eines elektronischen Münzdatensatzes (oder des Teils des elektronischen Münzdatensatzes) aus einem maskierten elektronischen Münzdatensatz ist dabei - äquivalent zur Erzeugung des privaten
20 Schlüssels aus einem öffentlichen Schlüssel in einem Verschlüsselungsverfahren über eine Restklassengruppe – sehr zeitintensiv. Wenn im vorliegenden Dokument von Summen und Differenzen oder anderen mathematischen Operationen die Rede ist, dann sind dabei im mathematischen Sinn die jeweiligen Operationen auf der entsprechenden mathematischen Gruppe zu verstehen, beispielsweise der Gruppe der Punkte auf einer elliptischen Kurve.

25 Die Einwegfunktion ist in einer Ausgestaltung homomorph, also ein kryptographisches Verfahren, welches über Homomorphie-Eigenschaften verfügt. Somit können mit dem maskierten elektronischen Münzdatensatz mathematische Operationen durchgeführt werden, die parallel dazu auch auf dem (unmaskierten) elektronischen Münzdatensatz durchgeführt und somit
30 nachvollzogen werden können. Mit Hilfe der homomorphen Einwegfunktion können Berechnungen mit maskierten elektronischen Münzdatensätzen in der Überwachungsinstanz nachvollzogen werden, ohne dass die entsprechenden (unmaskierten) elektronischen Münzdatensätze dort bekannt sind. Daher können bestimmte Berechnungen mit elektronischen Münzdatensätzen, beispielsweise für ein Modifizieren des (unmaskierten) elektronischen
35 Münzdatensatzes (zum Beispiel Aufteilen oder Verbinden), auch parallel mit den dazugehörigen maskierten elektronischen Münzdatensätzen nachgewiesen werden, beispielsweise zu Validierungsprüfungen oder zur Überwachung über die Rechtmäßigkeit des jeweiligen elektronischen Münzdatensatzes. Die Homomorphie-Eigenschaften treffen zumindest auf Additions- und Subtraktionsoperationen zu, sodass ein Aufteilen oder Kombinieren (=Verbinden)

von elektronischen Münzdatensätzen auch mittels der entsprechend maskierten elektronischen Münzdatensätze in der Überwachungsinstanz festgehalten und von anfragenden Endgeräten und/oder von der Überwachungsinstanz nachvollzogen werden kann, ohne Kenntnis über den monetären Betrag und das durchführende Endgerät zu erlangen.

5 Die Homomorphie-Eigenschaft ermöglicht es also, eine Eintragung von gültigen und ungültigen elektronischen Münzdatensätzen auf Basis ihrer maskierten elektronischen Münzdatensätze in einer Überwachungsinstanz zu führen ohne Kenntnis der elektronischen Münzdatensätze, auch wenn diese elektronische Münzdatensätze modifiziert werden (aufgeteilt, verbunden, umschalten).
10 Dabei wird sichergestellt, dass kein zusätzlicher monetärer Betrag geschaffen wurde oder dass eine Identität des Endgeräts in der Überwachungsinstanz festgehalten wird. Das Maskieren ermöglicht ein hohes Maß an Sicherheit, ohne einen Einblick in den monetären Betrag oder das Endgerät zu geben. Somit ergibt sich ein zweischichtiges Bezahlungssystem. Zum einen existiert die Verarbeitungsschicht, in der maskierte elektronische Datensätze geprüft werden, und zum anderen
15 die Direkttransaktionsschicht, in der zumindest zwei Endgeräte elektronische Münzdatensätze übertragen werden.

In einer weiteren Ausgestaltung ist die Einwegfunktion eine kryptographische Verschlüsselungsfunktion.

20 Das Anwenden der Einwegfunktion auf den elektronischen Münzdatensatz umfasst auch das Anwenden der Einwegfunktion auf einen Teil des elektronischen Münzdatensatzes, insbesondere auf den Verschleierungsbetrag und/oder einen Betragsteil des monetären Betrags, in einer Ausgestaltung nur auf den Verschleierungsbetrag (quasi-maskiert), in einer anderen Ausgestaltung
25 nur auf den ersten Betragsteil des monetären Betrags (teilbetragsmaskiert), in einer kombinierten Ausgestaltung auf eine Verknüpfung von Verschleierungsbetrag und erstem Betragsteils des monetären Betrags.

Das Erhalten des quasi-maskierten elektronischen Münzdatensatzes erfolgt unter Anwendung
30 einer kryptografischen Verschleierungsfunktion auf ein Münzdatensatzelement (bevorzugt den Verschleierungsbetrag) des (unmaskierten) elektronischen Münzdatensatzes. Der Verschleierungsbetrag (als Geheimelement) kann als ein dynamischer Schlüssel für eine Verschlüsselung verwendet werden. Der Verschleierungsbetrag kann nicht als ein Schlüssel für eine Entschlüsselung verwendet werden.

35 Beim Übertragen eines elektronischen Münzdatensatzes vom ersten Endgerät auf das zweite Endgerät haben zwei Endgeräte Kenntnis über den elektronischen Münzdatensatz. Um zu verhindern, dass das sendende erste Endgerät den elektronischen Münzdatensatz bei einem anderen (dritten) Endgerät ebenfalls zum Bezahlen verwendet (sogenanntes Double-Spending),

wird bevorzugt ein Umschalten („Switch“) des übertragenen elektronischen Münzdatensatzes vom ersten Endgerät auf das zweite Endgerät ausgeführt. Das Umschalten kann bevorzugt automatisch beim Empfangen eines elektronischen Münzdatensatzes im zweiten Endgerät geschehen. Zusätzlich kann es auch auf Anforderung, beispielsweise eines Befehls vom ersten und/ oder zweiten Endgerät, erfolgen. Zusätzlich kann ein elektronischer Münzdatensatz auch in zumindest zwei Münzteildatensätze aufgeteilt werden („Split“). Zusätzlich können zwei elektronische Münzdatensätze zu einem Münzdatensatz verbunden werden („Merge“).

Das Umschalten, das Aufteilen und das Verbinden sind verschiedene Modifikationen an einem elektronischen Münzdatensatz. Diese Modifikationen bedingen ein Registrieren des maskierten Münzdatensatzes in einer Überwachungsinstanz. Dieses Registrieren im Zuge der Modifikationen führt dazu, dass der vom ersten Endgerät gesendete elektronische Münzdatensatz ungültig wird und bei einem zweiten Ausgeben-Versuch des ersten Endgeräts als entsprechend ungültig erkannt wird. Der vom zweiten Endgerät zu registrierende Münzdatensatz wird durch das Registrieren in der Überwachungsinstanz gültig. Das konkrete Durchführen der einzelnen Modifikationen wird später erläutert.

Das Umschalten erfolgt zudem, wenn ein elektronischer Münzdatensatz modifiziert, beispielsweise aufgeteilt oder mit anderen elektronischen Münzdatensätzen verbunden wurde, insbesondere um einen zu zahlenden monetären Betrag passend begleichen zu können.

Für das Modifizieren von elektronischen Münzdatensätzen (Umschalten, Aufteilen, Verbinden) wird in der Überwachungsinstanz geprüft, ob der (maskierte) elektronische Münzdatensatz einen gültigen Bereich aufweist. Dazu werden sogenannte „Zero-Knowledge-Range-Proofs“ als Bereichsnachweise angewendet. Der Nachweis der Reichweite ermöglicht einerseits, dass ein geänderter monetärer Betrag (Aufteilen, Verbinden) innerhalb eines vordefinierten Bereichs gültiger monetärer Beträge ist und andererseits, dass das Eigentum an den zu ändernden monetären Beträgen nachgewiesen wird. Als ein Nachweis zählt die Darstellung des monetären Betrags im Binärformat und die darauf basierende Darstellung als Ringsignatur.

Diese Nachweis-Führung bedingt ein nicht geringes Datenvolumen auszutauschender Daten zwischen Endgerät und Überwachungsinstanz und einen Rechenaufwand. Wünschenswert ist es, dass derartige Nachweise wesentlich vereinfacht durchgeführt werden können.

Im erfindungsgemäßen Verfahren ist daher ein verbessertes Maskieren des zumindest einen elektronischen Münzdatensatzes vorgesehen, um die Bereichsnachweise zu vereinfachen.

Erfindungsgemäß wird vor dem Übertragen- und/oder vor dem Registrieren-Schritt eine Auswahl eines Maskierungsmodus getroffen beziehungsweise ein Maskierungsmodus festgelegt. Die

Auswahl erfolgt beispielsweise durch einen Benutzer des ersten Endgeräts über eine entsprechende Menüsteuerung am Endgerät. Die Auswahl erfolgt beispielsweise aufgrund einer Systemvorgabe im Bezahlssystem oder einer Systemvorgabe durch einen Drittanbieter. Beispielsweise kann so eine Leistungsfähigkeit des Bezahlsystems optimal ausgenutzt werden, sodass ein Aufwand der Nachweisprüfung auf Basis eines aktuellen Registrierer-Anfragevolumens in der Überwachungsinstanz durch entsprechende Auswahl des Maskierungsmodus gesteuert werden kann. Die Auswahl kann auch auf Basis einer Endgeräte-Eigenschaft gewählt werden. Beispielsweise bei fehlender Unterstützung eines der Maskierungsmodi, kann eine entsprechende Vorauswahl getroffen werden.

Entsprechend der Auswahl durch das Endgerät wird beim Registrieren in der Überwachungsinstanz eine Bereichsprüfung (= Range Proof) erstellt. Dazu gehört auch die stellenwertweise Darstellung des monetären Betrags zu einer beliebigen Basis, beispielsweise zur Basis 2 (binär) oder der Basis 3 (ternär), etc.

Durch die verschiedenen Maskierungsmodi lassen sich verschiedene Bereichsprüfungsoptionen realisieren:

Beispielsweise erfolgt keine Vereinfachung (Verkürzung) des Bereichsnachweises, wenn diese Option im System, bei der Überwachungsinstanz oder dem Endgerät nicht implementiert ist. Sodann erfolgt der Nachweis über den gesamten Bereich des monetären Betrags.

Alternativ ist die Bereichsnachweisvereinfachung gemäß einem festen Vorgabewert bei einer Modifikation (Umschalten, Aufteilen, Verbinden) eines Münzdatensatzes zwingend im System vorgeschrieben.

Alternativ ist die Bereichsnachweisverkürzung optional mit einem festen Vorgabewert vorgesehen. Dabei kann die Überwachungsinstanz festlegen, ob ein vollständig maskierter elektronischer Münzdatensatz oder ein quasimaskierter elektronischer Münzdatensatz oder ein teilbetragsmaskierter elektronischer Münzdatensatz zu erzeugen ist und ob ein Wechsel von einer Maskierungsart in eine andere Maskierungsart vorgenommen werden soll.

Alternativ ist die Bereichsnachweisverkürzung optional mit einem variablen Vorgabewert. Dabei kann der Anwender innerhalb der erlaubten Systemvorgaben festlegen, wieviel von dem maskierten Münzdatensatz offengelegt werden soll. Der variable Vorgabewert kann mit jeder Modifikation am Münzdatensatz wieder geändert werden.

Um die Leistungsfähigkeit des Verfahrens zu verbessern, wird im dritten Maskierungsmodus der Bereichsnachweis zusätzlich verkürzt, indem eine Ringsignatur nur auf den ersten monetären

Betragsteil angewendet wird, der einem Vorgabewert (Systemvorgabe oder Endgeräteauswahl) entspricht.

Die Entscheidung darüber, inwieweit Münzdatensatzelemente unmaskiert übertragen werden, also inwieweit beispielsweise Informationen über den elektronischen Münzdatensatz für eine Überwachungsinstanz transparent sind oder verborgen bleiben, könnte auf Basis einer Entscheidung der die jeweiligen Münzdatensätze übertragenden Endgeräte beruhen. Um dieses Aushandeln der Entscheidung zu beschreiben, werden die oben eingeführten Begriffe „vollständig maskierter Münzdatensatz“ und „unvollständig maskierter Münzdatensatz“ verwendet.

Dem vollständig maskierten Münzdatensatz ist ein (unmaskierter) privater elektronischer Münzdatensatz zugeordnet, welcher alle Münzdatensatzelemente, insbesondere den monetären Betrag, gegenüber der Überwachungsinstanz verbirgt. Für derartige private elektronische Münzdatensätze ist der zweite Maskierungsmodus zu wählen.

Dem teilbetragsmaskierten Münzdatensatz (im dritten Maskierungsmodus) ist ein (unmaskierter) halbprivater elektronischer Münzdatensatz zugeordnet, welcher den zweiten monetären Betragsteil gegenüber der Verifizierungsebene (Überwachungsinstanz) offenlegt. Für derartige halbprivate elektronische Münzdatensätze kann der dritte Maskierungsmodus gewählt werden.

Die Verwendung von privaten elektronischen Münzdatensätzen in einem Modifizieren-Schritt zusammen mit halbprivaten elektronischen Münzdatensätzen ist unproblematisch. Eine entsprechende Umschaltung eines privaten elektronischen Münzdatensatzes in einen halbprivaten elektronischen Münzdatensatz wird mit einem Umschalten-Schritt ermöglicht, wie es weiter unten beschrieben ist.

Der umgekehrte Fall, also das Verwenden von semiprivaten elektronischen Münzdatensätzen in einem Modifizieren-Schritt zusammen mit privaten elektronischen Münzdatensätzen, bedarf eines zusätzlichen Maskierungsschritts, wie er in einem Verbinden oder Aufteilen Schritt im zweiten Maskierungsmodus beschrieben ist.

Beim Verbinden zum Überführen eines halbprivaten in einen privaten elektronischen Münzdatensatz ist ein zusätzlicher privater elektronischer Münzdatensatz erforderlich. Ist momentan kein zusätzlicher privater elektronischer Münzdatensatz in dem jeweiligen Endgerät vorhanden, so wird ein privater elektronischer Nullmünzdatensatz verwendet, der einen monetären Betrag von null aber einen Verschleierungsbetrag aufweist, also keinen geldwerten Betrag darstellt. Dieser private Nullmünzdatensatz kann jederzeit aus einem einzigen vorhandenen privaten elektronischen Münzdatensatz mit einem Aufteilen-Schritt erstellt werden. In diesem

speziellen Aufteilen-Schritt wird ein erster privater Münzteildatensatz erzeugt, der den gleichen monetären Betrag aufweist, wie der einzig vorhandene private elektronische Münzdatensatz, und ein zweiter Münzteildatensatz wird erzeugt, der ein elektronischer Nullmünzdatensatz ist. Dieses Aufteilen zum Erhalten des privaten elektronischen Nullmünzdatensatz wird vor dem Überführen des halbprivaten in den privaten elektronischen Münzdatensatz durchgeführt und für die spätere Verwendung gespeichert.

Für das Registrieren im ersten oder dritten Maskierungsmodus wird beispielsweise der monetäre Betrag bzw. ein monetärer Betragsteil unmaskiert übertragen. Die entsprechenden Maskierungsmodi sind aber nicht auf das unmaskierte Übertragen des monetären Betrags(-teils) beschränkt, jedes andere Münzdatensatzelement(eitel) könnte alternativ oder zusätzlich unmaskiert übertragen werden. Dadurch wird das Senden zusätzlicher Datenpakete für komplexe Bereichsnachweise nicht mehr notwendig beziehungsweise steigt die Leistungsfähigkeit im vierten Maskierungsmodus durch die Verwendung wesentlich kleinerer Datenpakete.

Wenn die monetären Beträge (bzw. Betragsteile) unmaskiert bzw. unverschleiert übertragen werden, vereinfacht sich der Bereichsnachweis zu nur noch zwei Prüfschritten, nämlich (1), ob der dem unvollständig maskierten elektronischen Münzdatensatz hinzugefügte monetäre Betrag zu diesem maskierten elektronischen Münzdatensatz gehört und (2) ob das Eigentum der modifizierten (unmaskierten) elektronischen Münzdatensatz bewiesen ist. Im dritten Maskierungsmodus muss nur ein verkürzter Bereichsnachweis geprüft werden.

Der Hinzufügen-Schritt im ersten oder dritten Maskierungsmodus ist bevorzugt eine einfache logische Operation, beispielsweise eine Verkettung (Konkatenation) oder das Verwenden einer erweiterbaren Datenstruktur, beispielsweise einer TLV-Datenstruktur.

Diese Vereinfachungen bewirken Veränderungen in der Bereichsprüfung für die Modifikationen (Aufteilen, Verbinden, Umschalten), wie nachfolgend erläutert wird.

In einer bevorzugten Ausgestaltung des Verfahrens sind im zweiten Endgerät nach dem Übertragen die weiteren Verfahrensschritte vorgesehen: Umschalten des elektronischen Münzdatensatzes unter Generieren eines umzuschaltenden elektronischen Münzdatensatzes im Endgerät aus dem elektronischen Münzdatensatzes, wobei ein Verschleierungsbetrag für den umzuschaltenden elektronischen Münzdatensatz unter Verwendung des Verschleierungsbetrags des elektronischen Münzdatensatzes im zweiten Endgerät erzeugt wird; und der monetäre Betrag des elektronischen Münzdatensatzes als ein monetärer Betrag für den umzuschaltenden elektronischen Münzdatensatz verwendet wird.

Alternativ oder zusätzlich wird vorgesehen: Ein Aufteilen des elektronischen Münzdatensatzes in einen ersten elektronischen Münzteildatensatz und einen zweiten elektronischen Münzteildatensatz im ersten Endgerät, wobei der monetäre Betrag in wenigstens einen ersten monetären Betrag und einen zweiten monetären Betrag aufgeteilt wird.

5

Alternativ oder zusätzlich wird vorgesehen: Verbinden eines ersten und eines zweiten elektronischen Münzdatensatzes zu einem verbundenen elektronischen Münzdatensatzes im ersten Endgerät mit den Schritten: Berechnen eines Verschleierungsbetrags für den zu verbindenden elektronischen Münzdatensatz durch Bilden der Summe aus den jeweiligen Verschleierungsbeträgen des ersten und des zweiten elektronischen Münzdatensatzes; und Berechnen des monetären Betrags für den zu verbindenden elektronischen Münzdatensatz durch Bilden der Summe aus den jeweiligen monetären Beträgen des ersten und des zweiten elektronischen Münzdatensatzes.

10

15

Bei allen drei beschriebenen Verfahrensschritten, also dem Umschalten, dem Aufteilen und dem Verbinden, umfasst das Maskieren des elektronischen Münzdatensatzes im Maskieren-Schritt des zweiten Maskierungsmodus das Maskieren des umzuschaltenden Münzdatensatzes des ersten und/oder zweiten Münzteildatensatzes und/oder des verbundenen Münzdatensatzes.

20

Beim Maskieren des elektronischen Münzdatensatzes im Maskieren-Schritt des ersten oder dritten Maskierungsmodus wird ein Münzdatensatzelement, beispielsweise der Verschleierungsbetrag des jeweiligen elektronischen Münzdatensatzes als dynamischer privater Schlüssel genutzt, mit dem aber kein Entschlüsseln möglich ist.

25

Anschließend erfolgt für alle Maskierungsmodi ein Senden des vollständig maskierten elektronischen Münzdatensatzes oder des quasimaskierten elektronischen Münzdatensatzes oder des teilbetragsmaskierten elektronischen Münzdatensatzes an die Überwachungsinstanz zum Prüfen der Validität des elektronischen Münzdatensatzes durch die Überwachungsinstanz. Das Prüfen der Validität wird weiter unten im Detail erläutert.

30

In einer bevorzugten Ausgestaltung hat das Verfahren die weiteren Verfahrensschritte: Erzeugen einer Signatur unter Verwendung des Verschleierungsbetrags des elektronischen Münzdatensatzes; Hinzufügen der Signatur zu dem quasi-maskierten elektronischen Münzdatensatz oder dem vollständig maskierten elektronischen Münzdatensatz, wobei in der Überwachungsinstanz der vollständig maskierten elektronischen Münzdatensatz oder der quasimaskierte elektronische Münzdatensatz mit der Signatur registriert wird. In dieser Ausgestaltung wird die erstellte Signatur in der Überwachungsinstanz mit registriert.

35

In einer alternativen Ausgestaltung hat das Verfahren die weiteren Verfahrensschritte: Erzeugen einer Signatur unter Verwendung des Verschleierungsbetrags des elektronischen Münzdatensatzes; und Senden der Signatur zusammen mit dem quasi-maskierten elektronischen Münzdatensatz oder dem teilbetragsmaskierten elektronischen Münzdatensatz, wobei in der Überwachungsinstanz nur der teilbetragsmaskierte elektronische Münzdatensatz oder der quasimaskierte elektronische Münzdatensatz registriert wird.

In einer bevorzugten Ausgestaltung dieser Alternative hat das Verfahren registriert die Überwachungsinstanz nur teilbetragsmaskierte oder quasimaskierte elektronische Münzdatensatz und/oder nur elektronische Münzdatensätze, die zumindest für einen Betragsanteil betragsoffen sind.

In dieser alternativen Ausgestaltung wird die erstellte Signatur zum Übertragen des maskierten Münzdatensatzes zwischen Endgerät und Überwachungsinstanz verwendet, die Signatur wird aber nicht in der Überwachungsinstanz registriert – die Signatur ist kein Bestandteil des registrierten maskierten Münzdatensatzes. Die Signatur ist hier eine Transportsicherung und wird nach der Überprüfung verworfen, um den maskierten Münzdatensatz ohne Signatur zu registrieren.

Bevorzugt umfasst - nach dem Schritt des Umschaltens - der Registrieren-Schritt in der Überwachungsinstanz für den ersten Maskierungsmodus: Empfangen des quasimaskierten umzuschaltenden elektronischen Münzdatensatzes in der Überwachungsinstanz; Prüfen des quasimaskierten elektronischen Münzdatensatzes auf Validität in der Überwachungsinstanz; Prüfen, ob der monetäre Betrag des elektronischen Münzdatensatzes gleich dem monetären Betrags des umzuschaltenden elektronischen Münzdatensatzes ist; Berechnen der Differenz aus dem quasimaskierten umzuschaltenden Münzdatensatzes und dem quasimaskierten elektronischen Münzdatensatzes; Prüfen mit Hilfe einer Hinzugefügten Signatur, die durch Erzeugen eines öffentlichen Verifikationsschlüssels erstellt wurde; und Registrieren des quasimaskierten umzuschaltenden elektronischen Münzdatensatzes in der Überwachungsinstanz, wenn alle Prüfen-Schritte erfolgreich sind, wodurch der umzuschaltende elektronische Münzdatensatz als gültig gilt.

Bevorzugt umfasst - nach dem Schritt des Aufteilens - der Registrieren-Schritt in der Überwachungsinstanz für den zweiten und/oder dritten Maskierungsmodus: Empfangen der vollständig maskierten elektronischen Münzteildatensätze oder der teilbetragsmaskierten elektronischen Münzteildatensätze in der Überwachungsinstanz; Prüfen des maskierten umzuschaltenden elektronischen Münzdatensatzes auf Validität in der Überwachungsinstanz; Prüfen einer, den teilbetragsmaskierten elektronischen Münzteildatensätzen hinzugefügten Ringsignatur unter Verwendung des monetären Betrags des elektronischen Münzdatensatzes in der Überwachungsinstanz; Berechnen der Differenz aus der Summe der vollständig maskierten elektronischen Münzdatensätze oder der Summe der teilbetragsmaskierten elektronischen

- Münzteildatensätze und dem maskierten Münzdatensatz zum Prüfen, ob der monetäre Betrag des elektronischen Münzdatensatzes gleich der Summe aus erstem und zweitem monetären Betrag der jeweiligen elektronischen Münzteildatensätze ist - zum Prüfen, ob der monetäre Betrag des elektronischen Münzdatensatzes gleich dem monetären Betrags des umzuschaltenden elektronischen Münzdatensatzes ist; und Registrieren der maskierten elektronischen Münzteildatensätze in der Überwachungsinstanz, wenn alle Prüfen-Schritte erfolgreich sind und ein vereinfachter Bereichsnachweis erfolgt ist, wodurch die elektronischen Münzteildatensätze als gültig gelten.
- 10 Bevorzugt umfasst - nach dem Schritt des Verbindens - der Registrieren-Schritt in der Überwachungsinstanz für den zweiten und/oder den dritten Maskierungsmodus: Empfangen des teilbetragsmaskierten verbundenen elektronischen Münzdatensatz oder des vollständig maskierten verbundenen elektronischen Münzdatensatz in der Überwachungsinstanz; Prüfen der maskierten ersten und zweiten elektronischen Münzdatensätze auf Validität in der Überwachungsinstanz;
- 15 Prüfen einer ersten, dem teilbetragsmaskierten elektronischen Münzdatensatz oder dem vollständig maskierten elektronischen Münzdatensatz hinzugefügten Ringsignatur unter Verwendung des ersten monetären Betrags des ersten elektronischen Münzdatensatzes in der Überwachungsinstanz; Prüfen einer zweiten, dem teilbetragsmaskierten elektronischen Münzdatensatz oder dem vollständig maskierten elektronischen Münzdatensatz hinzugefügten
- 20 Ringsignatur unter Verwendung des zweiten monetären Betrags des zweiten elektronischen Münzdatensatzes in der Überwachungsinstanz; Berechnen der Differenz aus dem teilbetragsmaskierten verbundenen elektronischen Münzdatensatz oder dem vollständig maskierten verbundenen elektronischen Münzdatensatz und der Summe aus maskiertem ersten elektronischen Münzdatensatz und maskiertem zweiten elektronischen Münzdatensatz zum
- 25 Prüfen, ob der monetäre Betrag des verbundenen elektronischen Münzdatensatzes gleich der Summe aus dem ersten und dem zweiten monetären Betrag der ersten und zweiten elektronischen Münzdatensätze ist; Registrieren des maskierten verbundenen elektronischen Münzdatensatzes in der Überwachungsinstanz, wenn alle Prüfen-Schritte erfolgreich sind und ein vereinfachter Bereichsnachweis erfolgt ist, wodurch der verbundene elektronische Münzdatensatz als gültig gilt.
- 30 Bevorzugt umfasst - nach dem Schritt des Verbindens - der Registrieren-Schritt in der Überwachungsinstanz für den ersten Maskierungsmodus: Empfangen des quasi-maskierten verbundenen elektronischen Münzdatensatz in der Überwachungsinstanz; Prüfen der maskierten ersten und zweiten elektronischen Münzdatensätze auf Validität in der Überwachungsinstanz;
- 35 Prüfen einer ersten, dem quasi-maskierten elektronischen Münzdatensatz hinzugefügten Signatur durch Erzeugen eines ersten öffentlichen Verifikationsschlüssels in der Überwachungsinstanz; Prüfen einer zweiten, dem quasi-maskierten elektronischen Münzdatensatz hinzugefügten Signatur durch Erzeugen eines zweiten öffentlichen Verifikationsschlüssels in der Überwachungsinstanz; Berechnen der Differenz aus dem monetären Betrag des gültig zu

setzenden Münzdatensatzes und der Summe aus den monetären Beträge des zu verbindenden ersten elektronischen Münzdatensatzes und des zweiten elektronischen Münzdatensatzes; Registrieren des quasi-maskierten verbundenen elektronischen Münzdatensatzes in der Überwachungsinstanz, wenn alle Prüfen-Schritte erfolgreich sind und ein vereinfachter Bereichsnachweis erfolgt ist, wodurch der verbundene elektronische Münzdatensatz als gültig gilt.

Bevorzugt umfasst das Verfahren gemäß dem dritten Maskierungsmodus einen Schritt des Erstellens eines Nachweises im ersten Endgerät, wobei der Nachweis eine Information umfasst, dass der monetäre Betrag des elektronischen Münzdatensatzes positiv ist und dem Ersteller des Nachweises bekannt ist, nachfolgend auch vereinfachter Bereichsnachweis genannt, mit: Aufteilen des elektronischen Münzdatensatzes im ersten Endgerät entsprechend eines festen oder variablen Vorgabewertes, in einen ersten elektronischen Münzteildatensatz und einen zweiten elektronischen Münzteildatensatz; stellenwertweises Aufteilen des zweiten elektronischen Münzteildatensatzes im ersten Endgerät, wobei ein Stellenwert des aufgeteilten zweiten elektronischen Münzteildatensatzes ein Stellenwert des zweiten monetären Betrags des elektronischen Münzdatensatzes repräsentiert und die Summe aller Verschleierungsbeträge des stellenwertweise aufgeteilten zweiten elektronischen Münzdatensatzes den Verschleierungsbetrag des elektronischen Münzdatensatzes ergibt, wobei die Basis des Stellenwerts beliebig ist.

Basierend auf der stellenwertweisen Aufteilung des zweiten elektronischen Münzdatensatzes erstellt das Endgerät eine Ringsignatur, die zusammen mit dem teilbetragsmaskierten elektronischen Münzdatensatz an die Überwachungseinheit gesendet wird und dort geprüft wird.

Bevorzugt ist die Basis des Stellenwerts zwei oder drei. Mit Stellenwert wird eine Potenz der Basis eines Stellenwertsystems bezeichnet. So ist ein Binärsystem, ein Stellenwertsystem mit der Basis 2, ein Ternärsystem ist ein Stellenwertsystem mit der Basis 3 und ein Dezimalsystem ist ein Stellenwertsystem mit der Basis 10. Der Wert der Basis ist dabei nicht festgelegt, um ein möglichst flexibles stellenwertbasiertes Aufteilen für eine vereinfachte Nachweisprüfung zu ermöglichen.

Beispielsweise erfolgt das stellenwertweise Aufteilen auf Basis eines Vorgabewertes. Dieser Vorgabewert gibt beispielsweise die Stelle an, an der der monetäre Betrag aufzuteilen ist. Er entspricht dann beispielsweise einer Anzahl von „least significant bits, LSB“, wenn der Stellenwert die Basis 2 hat. Diese Anzahl LSB wird dann als zweiter monetärer Betragsteil dem teilmaskierten Münzdatensatz hinzugefügt. Die übrigen Stellen des monetären Betrags bilden den ersten monetären Betragsteil und ersetzen für den Maskieren-Schritt den monetären Betrag.

Dieser Vorgabewert entspricht alternativ beispielsweise einer Anzahl von „most significant bits, MSB“, wenn der Stellenwert die Basis 2 hat. Diese Anzahl MSB wird dann als zweiter monetärer Betragsteil dem teilmaskierten Münzdatensatz hinzugefügt. Die übrigen Stellen des monetären

Betrags bilden den ersten monetären Betragsteil und ersetzen für den Maskieren-Schritt den monetären Betrag.

5 Dieser Vorgabewert entspricht alternativ beispielsweise einer zufälligen Anzahl von Bits, wenn der Stellenwert die Basis 2 hat. Diese Anzahl von Bits wird dann als zweiter monetärer Betragsteil dem teilmaskierten Münzdatensatz hinzugefügt. Die übrigen Stellen des monetären Betrags bilden den ersten monetären Betragsteil und ersetzen für den Maskieren-Schritt den monetären Betrag.

10 Dieser Vorgabewert entspricht alternativ beispielsweise einer konkreten Auswahl von Bits, wenn der Stellenwert die Basis 2 hat. Diese Auswahl von Bits wird dann als zweiter monetärer Betragsteil dem teilmaskierten Münzdatensatz hinzugefügt. Die übrigen Stellen des monetären Betrags bilden den ersten monetären Betragsteil und ersetzen für den Maskieren-Schritt den monetären Betrag.

15 Der Überprüfungen werden bevorzugt Ringsignaturen zu Grunde gelegt, deren Parameter das Erzeugen von Zufallszahlen und dem Ableiten von Streuwerten (Hash) in den Endgeräten erfordert.

20 Ein für das Nachweisen definierter Vorgabewert kann – wie oben beschrieben – ein systembedingter Parameter oder das Ergebnis einer Aushandlung zwischen zwei Systemteilnehmern (Endgeräte oder Überwachungsinstanz) sein.

Nachfolgende Erläuterungen erfolgen in Bezug auf den ersten Maskierungsmodus und den dabei erstellten quasimaskierten Münzdatensätzen. Eine Voraussetzung zur Auswahl des ersten Maskierungsmodus könnte sein, dass im System keine Notwendigkeit besteht, ein Münzdatensatzelement, beispielsweise den monetären Betrag, zu maskieren (zu verstecken). Diese fehlende Notwendigkeit vereinfacht das gesamte Bezahlssystem und das Verfahren zum direkten Austausch von elektronischen Münzdatensätzen zwischen Endgeräten enorm. Einem elektronischen Münzdatensatz, wie oben beschrieben und mindestens einen monetären Betrag und einen Verschleierungsbetrag als Datenelemente umfassend, kann dann ein quasimaskierter elektronischer Münzdatensatz zugeordnet werden, der beispielsweise aus dem unmaskierten monetären Betrag und dem verschlüsselten Verschleierungsbetrag (=maskiertes Münzdatensatzelement) besteht. Alle Modifizierungen (Aufteilen, Umschalten, Verbinden) können auch auf diese quasimaskierten elektronischen Münzdatensätze angewendet werden und werden im Rahmen des ersten Maskierungsmodus hiernach abgehandelt. Die Ausführungen zum ersten Maskierungsmodus können alternative Ausgestaltungen zum zweiten oder dritten Maskierungsmodus darstellen, sie können aber hinsichtlich Signaturerstellung, Wahl der Verschlüsselungen, Wahl der Nachweisprüfungen beliebig miteinander kombiniert werden.

Generelles Ziel auch bei einer Kombination ist es, eine wesentliche Vereinfachung der Bereichsprüfungen (range-proofs) zu erhalten.

5 Bevorzugt erfolgt - nach dem Schritt des Umschaltens - der Registrieren-Schritt in der Überwachungsinstanz für den ersten Maskierungsmodus mit: Empfangen des quasi-maskierten umzuschaltenden elektronischen Münzdatensatzes in der Überwachungsinstanz; Prüfen des quasi-maskierten elektronischen Münzdatensatzes auf Validität in der Überwachungsinstanz; Prüfen einer, dem quasi-maskierten elektronischen Münzdatensatz hinzugefügten Signatur unter Verwendung des verschlüsselten Verschleierungsbetrags (=maskiertes Münzdatensatzelement)
10 des elektronischen Münzdatensatzes in der Überwachungsinstanz; und Registrieren des quasi-maskierten umzuschaltenden elektronischen Münzdatensatzes in der Überwachungsinstanz wenn die beiden Prüfen-Schritte erfolgreich sind, wodurch der umzuschaltende elektronische Münzdatensatz als gültig gilt.

15 Bevorzugt erfolgt - nach dem Schritt des Aufteilens - der Registrieren-Schritt in der Überwachungsinstanz für den ersten Maskierungsmodus mit: Empfangen der quasi-maskierten elektronischen Münzteildatensätze in der Überwachungsinstanz; Prüfen des quasi-maskierten elektronischen Münzdatensatzes auf Validität in der Überwachungsinstanz; Prüfen einer, dem quasi-maskierten elektronischen Münzdatensatz hinzugefügten Signatur unter Verwendung des maskierten Verschleierungsbetrags in der Überwachungsinstanz; Prüfen, ob der monetäre Betrag
20 des elektronischen Münzdatensatzes gleich der Summe aus ersten und zweiten monetären Betrag der elektronischen Münzteildatensätze ist; Registrieren der quasimaskierten elektronischen Münzteildatensätze in der Überwachungsinstanz, wenn die drei Prüfen-Schritte erfolgreich sind, wodurch die elektronischen Münzteildatensätze als gültig gelten und der aufzuteilende
25 elektronische Münzdatensatz als ungültig.

Bevorzugt erfolgt - nach dem Schritt des Verbindens - der Registrieren-Schritt in der Überwachungsinstanz für den ersten Maskierungsmodus mit: Empfangen des quasi-maskierten verbundenen elektronischen Münzdatensatz in der Überwachungsinstanz; Prüfen der
30 quasimaskierten ersten und zweiten elektronischen Münzdatensätze auf Validität in der Überwachungsinstanz; Prüfen zweier, den zu verbindenden quasi-maskierten verbundenen elektronischen Münzdatensätzen hinzugefügten Signaturen unter Verwendung der maskierten Verschleierungsbeträge in der Überwachungsinstanz; Prüfen, ob der monetäre Betrag des verbundenen elektronischen Münzdatensatzes gleich der Summe aus dem ersten und dem zweiten
35 monetären Betrag der ersten und zweiten elektronischen Münzdatensätze ist; Registrieren des quasi-maskierten verbundenen elektronischen Münzdatensatzes in der Überwachungsinstanz, wenn die drei Prüfen-Schritte erfolgreich sind, wodurch der verbundene elektronische Münzdatensatz als gültig gilt und die zwei zu verbindenden elektronischen Münzdatensätze als ungültig.

Der Schritt des Prüfens der quasi-maskierten Münzdatensätze im Umschalten,- Aufteilen, - oder Verbinden-Schritt erfolgt entsprechend dem Prüfen der Validität.

- 5 Bevorzugt wird zu jedem quasi-maskierten elektronischen Münzdatensatz eine Signatur erstellt. Der private Signaturschlüssel ist bevorzugt der (unmaskierte) Verschleierungsbetrag des (unmaskierten) Münzdatensatzes.

10 Die Signatur wird beim Umschalten-Schritt bevorzugt über dem quasi-maskierten elektronischen Münzdatensatzes und dem verschlüsselten Verschleierungsbetrag des quasimaskierten umzuschaltenden elektronischen Münzdatensatzes erstellt.

15 Die Signatur wird beim Aufteilen-Schritt bevorzugt über den quasi-maskierten elektronischen Münzdatensatz, den quasi-maskierten ersten elektronischen Münzteildatensatz und den quasimaskierten zweiten elektronischen Münzteildatensatz erstellt.

20 Die Signatur wird beim Verbinden-Schritt bevorzugt über den quasi-maskierten ersten elektronischen Münzdatensatz, den quasi-maskierten zweiten elektronischen Münzdatensatz und den quasimaskierten verbundenen elektronischen Münzdatensatz erstellt.

Für das Erstellen eines unmaskierten elektronischen Münzdatensatz für den ersten Maskierungsmodus wird eine Signatur des Herausgebers über den quasi-maskierten elektronischen Münzdatensatz in der Überwachungsinstanz hinterlegt.

- 25 Das Löschen eines quasi-maskierten elektronischen Münzdatensatzes erfolgt, wenn die Überwachungsinstanz die Signatur einer Herausgeberinstanz geprüft hat.

30 Die in diesem Verfahren erzeugten Signatur ersetzen eine ansonsten benötigte zusätzliche Informationen zum Führen eines Bereichsnachweis über den maskierten aufzuteilenden elektronischen Münzdatensatz bzw. einen Bereichsnachweis über jeweilig maskierte elektronische Münzteildatensätze.

35 Zum Erzeugen der Signatur wird bevorzugt ein asymmetrisches Kryptosystem, bei dem das Endgerät mit Hilfe eines geheimen Signaturschlüssels, nachfolgend auch privater Signaturschlüssel oder „Private Key“ bezeichnet, zu einem Münzdatensatz einen Wert berechnet. Dieser Wert ermöglicht es jedem, mit Hilfe eines öffentlichen Verifikationsschlüssels, dem Public Key, die Urheberschaft und Integrität des Münzdatensatzes zu prüfen.

Die in diesem Verfahren für den ersten Maskierungsmodus hinzugefügte Signatur ist beispielsweise eine erste Signatur und ein privater Signaturschlüssel zum Erzeugen der ersten Signatur ist der Verschleierungsbetrag des entsprechenden elektronischen Münzdatensatzes. Dementgegen werden für den zweiten Maskierungsmodus nur zwei Signaturen verwendet, nämlich die Signatur der Zentralbank zum Erzeugen und Löschen (=fixer privater Schlüssel) und die Signatur für das Umschalten (Verschleierungsbetrag als privater Schlüssel).

Die in diesem Verfahren (aller Maskierungsmodi) hinzugefügte Signatur ist beispielsweise eine zweite Signatur und ein privater Signaturschlüssel zum Erzeugen der zweiten Signatur wird aus einer Differenz aus dem Verschleierungsbetrag des elektronischen Münzdatensatzes und dem Verschleierungsbetrag für den umzuschaltenden elektronischen Münzdatensatz gebildet.

Ein öffentlicher Verifikationsschlüssel zum Prüfen der ersten Signatur wird bevorzugt aus einer Differenz aus dem maskierten elektronischen Münzdatensatz und einem Anwenden der kryptografischen Verschlüsselungsfunktion auf den monetären Betrag des elektronischen Münzdatensatzes gebildet.

Ein öffentlicher Verifikationsschlüssel zum Prüfen der zweiten Signatur wird bevorzugt aus einer Differenz aus dem umzuschaltenden maskierten elektronischen Münzdatensatz und dem maskierten elektronischen Münzdatensatz gebildet.

Das Verfahren weist bevorzugt die weiteren folgenden Schritte auf: Umschalten des übertragenen elektronischen Münzteildatensatzes; und/oder Verbinden des übertragenen elektronischen Münzdatensatzes mit einem zweiten elektronischen Münzdatensatz zu einem weiteren elektronischen Münzdatensatz, nämlich verbundenen elektronischen Münzdatensatz.

Beim Umschalten ergibt der vom ersten Endgerät erhaltene elektronische Münzteildatensatz einen neuen elektronischen Münzdatensatz, bevorzugt mit gleichem monetärem Betrag, dem sogenannten umzuschaltenden elektronischen Münzdatensatz. Der neue elektronische Münzdatensatz wird vom zweiten Endgerät generiert, vorzugsweise indem der monetäre Betrag des erhaltenen elektronischen Münzdatensatzes als monetärer Betrag des umzuschaltenden elektronischen Münzdatensatzes verwendet wird. Dabei wird ein neuer Verschleierungsbetrag, beispielsweise eine Zufallszahl, generiert. Der neue Verschleierungsbetrag wird beispielsweise zum Verschleierungsbetrag des erhaltenen elektronischen Münzdatensatzes addiert, damit die Summe beider Verschleierungsbeträge (neu und erhalten) als Verschleierungsbetrag des umzuschaltenden elektronischen Münzdatensatzes dient. Nach dem Umschalten wird bevorzugt der erhaltene elektronische Münzteildatensatz und der umzuschaltende elektronische Münzteildatensatz im Endgerät durch Anwenden der Einwegfunktion auf jeweils den erhaltenen elektronischen Münzteildatensatz und den umzuschaltenden elektronischen Münzteildatensatz

maskiert, um entsprechend einen maskierten erhaltenen elektronischen Münzteildatensatz und einen maskierten umzuschaltenden elektronischen Münzteildatensatz zu erhalten.

5 Neu geschaffene Verschleierungsbeträge müssen eine hohe Entropie aufweisen, da sie als Blendungsfaktor für die entsprechenden maskierten elektronischen Münzteildatensätze verwendet werden. Bevorzugt wird dazu ein Zufallszahlengenerator auf dem Endgerät verwendet.

10 Bislang wurden im Rahmen des Umschaltens bevorzugt zusätzliche Informationen, die zum Registrieren des Umschaltens des maskierten elektronischen Münzdatensatzes in der entfernten Überwachungsinstanz benötigt werden, im Endgerät berechnet. Bevorzugt beinhalten die zusätzlichen Informationen einen Bereichsnachweis über den maskierten umzuschaltenden elektronischen Münzdatensatz und einen Bereichsnachweis über den maskierten erhaltenen elektronischen Münzdatensatz. Bei dem Bereichsnachweis handelt es sich um einen Nachweis, dass der monetäre Betrag des elektronischen Münzdatensatzes nicht negativ ist, der elektronische Münzdatensatz gültig erstellt und/ oder der monetäre Betrag und der Verschleierungsbetrag des elektronischen Münzdatensatzes dem Ersteller des Bereichsnachweises bekannt sind. Insbesondere dient der Bereichsnachweis dazu, diese(n) Nachweis(e) zu führen, ohne den monetären Wert und/oder den Verschleierungsbetrag des maskierten elektronischen Münzdatensatzes zu offenbaren. Diese Bereichsnachweise werden auch „Zero-Knowledge-Range-Proofs“ genannt. Bevorzugt werden als Bereichsnachweis Ringsignaturen verwendet. Anschließend erfolgt ein Registrieren des Umschaltens des maskierten elektronischen Münzdatensatzes in der entfernten Überwachungsinstanz.

25 Das Umschalten wird also durch Hinzufügen eines neuen Verschleierungsbetrags zum Verschleierungsbetrag des erhaltenen elektronischen Münzdatensatz abgesichert, wodurch ein Verschleierungsbetrag erhalten wird, den nur das zweite Endgerät kennt. Neu geschaffene Verschleierungsbeträge müssen aber eine hohe Entropie aufweisen, da sie als Blendungsfaktor für die entsprechenden maskierten elektronischen Münzteildatensätze verwendet werden. Bevorzugt wird dazu ein Zufallszahlengenerator auf dem Endgerät verwendet. Diese Absicherung kann in der Überwachungsinstanz nachverfolgt werden.

35 Weiterhin umfasst das Verfahren die nachfolgenden Schritte: Maskieren des umzuschaltenden elektronischen Münzteildatensatzes im zweiten Endgerät durch Anwenden der beispielsweise homomorphen Einwegfunktion auf den umzuschaltenden elektronischen Münzteildatensatz zum Erhalten eines maskierten elektronischen Münzdatensatzes; und Registrieren des maskierten elektronischen Münzdatensatzes in einer entfernten Überwachungsinstanz.

Die hier beschriebenen Schritte müssen nicht in der beschriebenen Reihenfolge durchgeführt werden. Die hier beschriebene Reihenfolge ist jedoch eine bevorzugte Ausgestaltung.

Der Schritt des Registrierens wird vorzugsweise dann ausgeführt, wenn das zweite Endgerät mit der Überwachungsinstanz verbunden ist. Während die elektronischen Münzdatensätze für direktes Bezahlen zwischen zwei Endgeräten verwendet werden, werden die maskierten Münzdatensätze in der Überwachungsinstanz registriert, wodurch Modifikationen an den maskierten elektronischen Münzdatensätzen in der Überwachungsinstanz registriert werden können.

In einer weiter bevorzugten Ausgestaltung des Verfahrens wird für ein Verbinden von elektronischen Münzteildatensätzen ein weiterer elektronischer Münzdatensatz (verbundener elektronischer Münzdatensatz) aus einem ersten und einem zweiten elektronischen Münzteildatensatz bestimmt. Dabei wird der Verschleierungsbetrag für den zu verbindenden elektronischen Münzdatensatz durch Bilden der Summe aus den jeweiligen Verschleierungsbeträgen des ersten und des zweiten elektronischen Münzdatensatzes berechnet. Weiterhin wird vorzugsweise der monetäre Betrag für den verbundenen elektronischen Münzdatensatz durch Bilden der Summe aus den jeweiligen monetären Beträgen des ersten und des zweiten elektronischen Münzdatensatzes berechnet.

Nach dem Verbinden wird der erste elektronische Münzteildatensatz, der zweite elektronische Münzteildatensatz, sowie der zu verbindende elektronische Münzdatensatz im (ersten und/ oder zweiten) Endgerät durch Anwenden der beispielsweise homomorphen Einwegfunktion auf jeweils den ersten elektronischen Münzteildatensatz, den zweiten elektronischen Münzteildatensatz, sowie den zu verbindenden elektronischen Münzdatensatz maskiert, um entsprechend einen maskierten ersten elektronischen Münzteildatensatz, einen maskierten zweiten elektronischen Münzteildatensatz, sowie einen maskierten zu verbindenden elektronischen Münzdatensatz zu erhalten. Des Weiteren werden zusätzliche Informationen, die zum Registrieren des Verbindens der maskierten elektronischen Münzdatensätze in der entfernten Überwachungsinstanz benötigt werden, im Endgerät berechnet. Bevorzugt beinhalten die zusätzlichen Informationen einen Bereichsnachweis über den maskierten ersten elektronischen Münzteildatensatz und einen Bereichsnachweis über den maskierten zweiten elektronischen Münzteildatensatz. Bei dem Bereichsnachweis handelt es sich um einen Nachweis, dass der monetäre Betrag des elektronischen Münzdatensatzes nicht negativ ist, der elektronische Münzdatensatz gültig erstellt und/ oder der monetäre Betrag und der Verschleierungsbetrag des elektronischen Münzdatensatzes dem Ersteller des Bereichsnachweises bekannt sind. Insbesondere dient der Bereichsnachweis dazu, diese(n) Nachweis zu führen ohne den monetären Wert und/oder den Verschleierungsbetrag des maskierten elektronischen Münzdatensatzes zu offenbaren. Diese Bereichsnachweise werden auch „Zero-Knowledge-Range-Proofs“ genannt. Bevorzugt werden als Bereichsnachweis Ringsignaturen verwendet. Anschließend erfolgt ein Registrieren des Verbindens der beiden maskierten elektronischen Münzteildatensätze in der entfernten Überwachungsinstanz.

Mit dem Schritt des Verbindens können zwei elektronische Münzdatensätze bzw. zwei elektronische Münzteildatensätze zusammengefasst werden. Dabei werden die monetären Beträge sowie auch die Verschleierungsbeträge addiert. Wie beim Aufteilen kann somit auch beim Verbinden eine Validität der beiden ursprünglichen Münzdatensätze durchgeführt werden.

5

In einer bevorzugten Ausgestaltung umfasst der Registrieren-Schritt das Empfangen des maskierten umzuschaltenden elektronischen Münzteildatensatzes in der Überwachungsinstanz, das Prüfen des maskierten umzuschaltenden elektronischen Münzteildatensatzes auf Validität; und das Registrieren des maskierten umzuschaltenden elektronischen Münzdatensatzes in der Überwachungsinstanz, wenn der Prüfen-Schritt erfolgreich ist, wodurch der umzuschaltende elektronische Münzteildatensatz als überprüft gilt.

Bevorzugt wird im Prüfen-Schritt festgestellt, ob die Differenz aus maskiertem elektronischem Münzdatensatz und maskiertem umzuschaltenden elektronischen Münzteildatensatz gleich einem öffentlichen Verifikationsschlüssel der Signatur ist. Dies ermöglicht das einfache Prüfen der Gültigkeit des Münzteildatensatzes ohne aufwendige Zero-Knowledge-Nachweise. Der Zero-Knowledge-Proof wird aber dennoch benötigt, um einen Besitz des elektronischen Münzdatensatzes zu beweisen (außer im ersten Maskierungsmodus).

Ein Hauptunterscheidungsmerkmal dieses Erfindungskonzepts gegenüber bekannten Lösungen ist, dass die Überwachungsinstanz nur (also ausschließlich) Kenntnis über die maskierten elektronischen Münzdatensätze/Münzteildatensätze und eine Liste mit Verarbeitungen bzw. Änderungen an dem maskierten elektronischen Münzdatensatz/Münzteildatensatz führt. Der tatsächliche Zahlungsverkehr mit den (unmaskierten) Münzdatensätzen/Münzteildatensätzen wird in der Überwachungsinstanz nicht registriert und findet in einer Direkttransaktionsschicht direkt zwischen Endgeräten statt.

Erfindungsgemäß ist auch ein zweischichtiges Bezahlungssystem aus einer Direktbezahltransaktionsschicht, zum direkten Austauschen von (unmaskierten) elektronischen Münzdatensätzen und einer Überwachungsschicht, welche die Datenbank umfasst, vorgesehen. In der Überwachungsinstanz, der Überwachungsschicht, werden keine Bezahltransaktionen festgehalten, sondern ausschließlich maskierte elektronische Münzdatensätze und deren Verarbeitungen zum Zweck der Verifizierung der Gültigkeit von (unmaskierten) elektronischen Münzdatensätzen. So wird die Anonymität der Teilnehmer des Bezahlungssystems gewährleistet. Die Überwachungsinstanz gibt Auskunft über gültige und ungültige elektronische Münzdatensätze, um beispielsweise eine Mehrfach-Ausgabe des gleichen elektronischen Münzdatensatzes zu vermeiden oder die Echtheit des elektronischen Münzdatensatzes als gültig herausgegebenes elektronisches Geld zu verifizieren.

Das Endgerät kann also in der Direktbezahltransaktionsschicht einem anderen Endgerät elektronische Münzdatensätze übertragen ohne Verbindung zur Überwachungsinstanz, insbesondere wenn das Endgerät offline ist, also keine Kommunikationsverbindung zu der Überwachungsinstanz vorhanden ist.

5

Das Endgerät kann vorliegend ein Sicherheitselement aufweisen, in dem die elektronischen Münzdatensätze sicher abgelegt sind. Ein Sicherheitselement ist bevorzugt ein spezielles Computerprogrammprodukt, insbesondere in Form einer abgesicherten Laufzeitumgebung innerhalb eines Betriebssystems eines Endgeräts, englisch Trusted Execution Environments, TEE, gespeichert auf einem Datenspeicher, beispielsweise eines mobilen Endgeräts, einer Maschine, vorzugsweise Bankautomat. Alternativ ist das Sicherheitselement beispielsweise als spezielle Hardware, insbesondere in Form eines gesicherten Hardware-Plattform-Moduls, englisch Trusted Platform Module, TPM oder als ein eingebettetes Sicherheitsmodul, eUICC, eSIM, ausgebildet. Das Sicherheitselement stellt eine vertrauenswürdige Umgebung bereit.

15

Die Kommunikation zwischen zwei Endgeräten kann drahtlos oder drahtgebunden, oder z.B. auch auf optischem Weg, bevorzugt über QR-Code oder Barcode, erfolgen und kann als ein gesicherter Kanal ausgebildet sein. Der optische Weg kann beispielsweise die Schritte des Generierens einer optischen Codierung, insbesondere einer 2D-Codierung, vorzugsweise ein QR-Code, und des Einlesens der optischen Codierung umfassen. Somit ist der Austausch des elektronischen Münzdatensatzes beispielsweise durch kryptografische Schlüssel gesichert, beispielsweise einem für einen elektronischen Münzdatensatz-Austausch ausgehandelten Sitzungsschlüssel oder einem symmetrischen oder asymmetrischen Schlüsselpaar.

20

25

Durch das Kommunizieren zwischen Endgeräten, beispielsweise über ihre Sicherheitselemente, werden die ausgetauschten elektronischen Münzdatensätze vor Diebstahl oder Manipulation geschützt. Die Ebene der Sicherheitselemente ergänzt so die Sicherheit etablierter Blockchain-Technologie.

30

In einer bevorzugten Ausgestaltung erfolgt das Übertragen der Münzdatensätze als APDU Kommandos. Dazu ist der Münzdatensatz bevorzugt in einer (embedded) UICC als Sicherheitselement abgelegt und wird dort verwaltet. Ein APDU ist ein kombinierter Kommando-/Datenblock eines Verbindungsprotokolls zwischen der UICC und einem Gerät. Die Struktur der APDU ist durch den Standard ISO-7816-4 definiert. APDUs stellen ein Informationselement der Anwendungsebene (Schicht 7 des OSI-Schichtenmodells) dar.

35

Darüber hinaus ist es vom Vorteil, dass die elektronischen Münzdatensätze in beliebiger Formatierung übertragen werden können. Dies impliziert, dass sie auf beliebigen Kanälen

kommuniziert, also übertragen werden können. Sie müssen nicht in einem festgelegten Format oder in einem bestimmten Programm gespeichert werden.

Als ein Endgerät wird insbesondere ein mobiles Telekommunikationsendgerät, beispielsweise ein Smartphone angesehen. Alternativ oder zusätzlich kann das Endgerät auch ein Gerät, wie Wearable, Smartcard, Maschine, Werkzeug, Automat oder auch Behälter bzw. Fahrzeug sein. Ein erfindungsgemäßes Endgerät ist somit entweder stationär oder mobil. Das Endgerät ist vorzugsweise ausgebildet, das Internet und/ oder andere öffentliche oder private Netze zu nutzen. Dazu verwendet das Endgerät eine geeignete Verbindungstechnologie, beispielsweise Bluetooth, Lora, NFC und/ oder WiFi und weist wenigstens eine entsprechende Schnittstelle auf. Das Endgerät kann auch ausgebildet sein, mittels Zugangs zu einem Mobilfunknetz mit dem Internet und/ oder anderen Netzen verbunden zu werden.

In einer Ausgestaltung kann vorgesehen sein, dass das erste und/ oder zweite Endgerät bei dem aufgezeigten Verfahren die empfangenen elektronischen Münzdatensätze bei Vorliegen oder Empfang mehrerer elektronischer Münzdatensätze diese entsprechend ihrer monetären Wertigkeit abarbeitet. So kann vorgesehen sein, dass elektronische Münzdatensätze mit höherer monetärer Wertigkeit vor elektronische Münzdatensätze mit niedriger monetärer Wertigkeit verarbeitet. In einer Ausgestaltung kann das erste und/ oder zweite Endgerät ausgebildet sein, nach Empfang eines elektronischen Münzdatensatzes diesen in Abhängigkeit von beigefügter Information, beispielsweise einer Währung oder Denomination, mit bereits im zweiten Endgerät vorhandenem elektronischen Münzdatensatz zu verbinden und entsprechend einen Schritt des Verbindens auszuführen. Weiterhin kann das zweite Endgerät auch zum automatisierten Ausführen eines Umschaltens nach Empfang des elektronischen Münzdatensatzes vom ersten Endgerät ausgebildet sein.

In einer Ausgestaltung werden beim Übertragen weitere Informationen, insbesondere Metadaten, vom ersten Endgerät auf das zweite Endgerät übermittelt, beispielsweise eine Währung. Diese Information kann in einer Ausgestaltung vom elektronischen Münzdatensatz umfasst sein.

In einer bevorzugten Ausgestaltung weist das Verfahren die folgenden weiteren Schritte auf: Maskieren des übertragenen elektronischen Münzdatensatzes im zweiten Endgerät durch Anwenden der beispielsweise homomorphen Einwegfunktion auf den übertragenen elektronischen Münzdatensatz; und Senden des maskierten übertragenen elektronischen Münzdatensatzes an die entfernte Überwachungsinstanz zum Prüfen der Validität des übertragenen elektronischen Münzdatensatzes durch die entfernte Überwachungsinstanz. In diesem Fall wurde beispielsweise der gesamte monetäre Betrag im Rahmen des elektronischen Münzdatensatzes an das zweite Endgerät übertragen. Bevor ein Zahlungsempfänger diesen elektronischen Münzdatensatz akzeptiert, überprüft er gegebenenfalls dessen Gültigkeit. Zu diesem Zweck erzeugt das zweite

Endgerät den maskierten übertragenen elektronischen Münzdatensatz, sendet diesen zur Überwachungsinstanz und fragt dabei bei der Überwachungsinstanz die Gültigkeit des elektronischen Münzdatensatzes ab. Die Überwachungsinstanz prüft nun, ob der maskierte übertragene elektronische Münzdatensatz überhaupt vorhanden ist und ob er weiterhin gültig ist, also nicht bereits durch ein anderes Endgerät verbraucht ist, um so Doppelausgaben zu vermeiden.

In einer Ausgestaltung wird im zweiten Endgerät ein Nachweis erstellt. Der Nachweis umfasst eine Information über die Übereinstimmung des monetären Betrags des übertragenen elektronischen Münzdatensatzes mit dem monetären Betrag des umzuschaltenden elektronischen Münzdatensatzes. Vorzugsweise umfasst der Nachweis lediglich eine Information über die Übereinstimmung, nicht aber einen der monetären Beträge.

Bevorzugt erfolgt während des Registrieren-Schrittes ein Verifizieren der elektronischen Münzdatensätze des ersten und/ oder zweiten Endgeräts in der bzw. durch die Überwachungsinstanz. Die Prüfung erfolgt in Abhängigkeit der der Verifikation vorangehenden Schritte, beispielsweise ob ein Schritt des Umschaltens, des Verbindens und/ oder des Aufteilens erfolgt ist. Dabei kann die Überwachungsinstanz beispielsweise die Gültigkeit der (maskierten) übertragenen und/oder aufzuteilenden und/oder ersten und zweiten elektronischen Münzdatensätzen prüfen. Dies ermöglicht es, festzustellen, ob die elektronischen Münzdatensätze zum ersten Mal verarbeitet werden. Falls die (maskierten) elektronischen Münzdatensätze nicht gültig sind (also insbesondere falls sie nicht in der Überwachungsinstanz vorliegen) kann das Registrieren nicht erfolgreich ausgeführt werden, zum Beispiel weil das Endgerät versucht einen elektronischen Münzdatensatz mehrfach auszugeben.

In einer weiter bevorzugten Ausgestaltung umfasst der Registrieren-Schritt nach dem Ausführen des Umschalten-Schritts beispielsweise das Versenden des vom Endgerät vorbereiteten Umschalten-Befehls an die Überwachungsinstanz. Bevorzugt teilt die Überwachungsinstanz das Ergebnis des Ausführens des Umschalten-Befehls dem „befehlenden“ Endgerät mit, d.h. welche der involvierten maskierten elektronischen Münzdatensätze nach Ausführen des Umschalten-Befehls gültig sind.

In einer bevorzugten Ausgestaltung ist die Überwachungsinstanz eine entfernte Instanz. Damit ist beispielsweise zum Registrieren des elektronischen Münzdatensatzes der Aufbau einer Kommunikationsverbindung zu der Überwachungsinstanz vorgesehen.

Die Überwachungsinstanz ist als übergeordnete Instanz ausgebildet. Die Überwachungsinstanz ist demnach nicht zwingend in der Ebene bzw. in der Schicht der Endgeräte (Direkttransaktionsschicht) angeordnet. Vorzugsweise ist die Überwachungsinstanz zur Verwaltung und Prüfung von maskierten elektronischen Münzdatensätzen vorgesehen und einer

Herausgeberschicht, in welcher auch eine Herausgeberinstanz angeordnet ist, und/ oder einer Überwachungsschicht angeordnet. Es ist denkbar, dass die Überwachungsinstanz zusätzlich Transaktionen zwischen Endgeräten verwaltet und prüft.

- 5 Die Überwachungsinstanz ist bevorzugt eine Datenbank, in der die maskierten elektronischen Münzdatensätze mit entsprechender Verarbeitung des maskierten elektronischen Münzdatensatzes registriert sind. Die Datenbank kann als dezentral gesteuerte Datenbank, englisch Distributed Ledger Technology (DLT), ausgestaltet sein. In einer bevorzugten Ausgestaltung lässt sich daraus ein Gültigkeitsstatus des (maskierten) elektronischen Münzdatensatzes ableiten. Bevorzugt wird
- 10 die Gültigkeit der (maskierten) elektronischen Münzdatensätze in der und durch die Überwachungsinstanz vermerkt. Die Registrierung der Verarbeitung bzw. der Verarbeitungsschritte kann auch das Registrieren von Prüfergebnissen und Zwischenprüfergebnissen betreffend die Gültigkeit eines elektronischen Münzdatensatzes betreffen. Ist eine Verarbeitung endgültig, wird dies beispielsweise durch entsprechende
- 15 Markierungen oder einer abgeleiteten Gesamtmarkierung angezeigt. Eine endgültige Verarbeitung entscheidet sodann, ob ein elektronischer Münzdatensatz gültig oder ungültig ist.

- Diese Datenbank ist weiter bevorzugt eine nicht-öffentliche Datenbank, kann aber auch als öffentliche Datenbank realisiert werden. Diese Datenbank ermöglicht es auf einfache Weise,
- 20 Münzdatensätze bezüglich ihrer Gültigkeit zu prüfen und „Double-Spending“, also Mehrfachausgaben, zu verhindern, ohne dass die Bezahltransaktion selbst registriert oder protokolliert wird. Die Datenbank beschreibt dabei eine Technik für vernetzte Computer, die zu einer Übereinkunft über die Reihenfolge von bestimmten Transaktionen kommen und darüber, dass diese Transaktionen Daten aktualisieren. Es entspricht einem dezentral geführten
- 25 Verwaltungssystem oder einer dezentral geführten Datenbank.

In einer weiteren Ausgestaltung kann die Datenbank auch als öffentliche Datenbank ausgebildet sein.

- 30 Alternativ ist die Überwachungsinstanz eine zentral geführte Datenbank, beispielsweise in Form eines öffentlich zugänglichen Datenspeichers oder als Mischform aus zentraler und dezentraler Datenbank.

- Bevorzugt wird der zumindest eine initiale elektronische Münzdatensatz ausschließlich von der
- 35 Herausgeberinstanz erstellt, wobei vorzugsweise die aufgeteilten elektronischen Münzdatensätze, insbesondere elektronischen Münzteildatensätze, auch durch ein Endgerät generiert werden können. Das Erstellen und das Wählen eines monetären Betrags beinhalten bevorzugt auch das Wählen eines Verschleierungsbetrags mit hoher Entropie. Die Herausgeberinstanz ist ein Rechensystem, welches bevorzugt entfernt vom ersten und/ oder zweiten Endgerät ist. Nach dem

Erstellen des neuen elektronischen Münzdatensatzes wird der neue elektronische Münzdatensatz in der Herausgeberinstanz durch Anwenden der beispielsweise homomorphen Einwegfunktion auf den neuen elektronischen Münzdatensatz maskiert, um entsprechend einen maskierten neuen elektronischen Münzdatensatz zu erhalten. Des Weiteren werden zusätzliche Informationen, die

5 zum Registrieren des Erstellens des maskierten neuen elektronischen Münzdatensatzes in der entfernten Überwachungsinstanz benötigt werden, in der Herausgeberinstanz berechnet. Bevorzugt sind diese weiteren Informationen ein Nachweis, dass der (maskierte) neue elektronische Münzdatensatz von der Herausgeberinstanz stammt, beispielsweise durch eine signieren des maskierten neuen elektronischen Münzdatensatzes. In einer Ausgestaltung kann

10 vorgesehen sein, dass die Herausgeberinstanz einen maskierten elektronischen Münzdatensatz beim Erzeugen des elektronischen Münzdatensatzes mit ihrer Signatur signiert. Die Signatur der Herausgeberinstanz wird dazu in der Überwachungsinstanz hinterlegt. Die Signatur der Herausgeberinstanz ist von der erzeugten Signatur des ersten Endgeräts verschieden.

15 Bevorzugt kann die Herausgeberinstanz einen elektronischen Münzdatensatz, der sich in ihrem Besitz befindet (also von dem sie den monetären Betrag und den Verschleierungsbetrag kennt) deaktivieren, indem sie den maskierten zu deaktivierenden elektronischen Münzdatensatz mit der beispielsweise homomorphen Einwegfunktion maskiert und einen Deaktivieren-Befehl für die Überwachungsinstanz vorbereitet. Teil des Deaktivieren-Befehls ist bevorzugt neben dem

20 maskierten zu deaktivierenden elektronischen Münzdatensatzes auch der Nachweis, dass der Deaktivieren Schritt von der Herausgeberinstanz initiiert wurde, beispielsweise in Form des signierten maskierten zu deaktivierenden elektronischen Münzdatensatzes. Als zusätzliche Information könnten im Deaktivieren-Befehl Bereichsprüfungen für den maskierten zu deaktivierenden elektronischen Münzdatensatz enthalten sein. Anschließend erfolgt ein

25 Registrieren des Deaktivierens des maskierten elektronischen Münzdatensatzes in der entfernten Überwachungsinstanz. Mit dem Deaktivieren-Befehl wird der Schritt des Deaktivierens ausgelöst.

Die Schritte Erstellen und Deaktivieren erfolgen bevorzugt an gesicherten Orten, insbesondere nicht in den Endgeräten. In einer bevorzugten Ausgestaltung werden die Schritte des Erstellens und Deaktivierens nur von der Herausgeberinstanz durchgeführt bzw. angestoßen. Vorzugsweise

30 finden diese Schritte an einen gesicherten Ort statt, beispielsweise in einer Hard- und Software-Architektur, die zur Verarbeitung von sensiblem Datenmaterial in unsicheren Netzen entwickelt wurde. Das Deaktivierendes entsprechenden maskierten elektronischen Münzdatensatz bewirkt, dass der entsprechende maskierte elektronische Münzdatensatz nicht mehr für weitere

35 Verarbeitung, insbesondere Transaktionen, verfügbar ist, da er in und von der Überwachungsinstanz als ungültig markiert wurde. Jedoch kann in einer Ausführungsform vorgesehen sein, dass der deaktivierte maskierte elektronische Münzdatensatz bei der Herausgeberinstanz archivarisch bestehen bleibt. Dass der deaktivierte maskierte elektronische Münzdatensatz nicht mehr gültig ist, kann beispielsweise mithilfe eines Flags oder einer anderen

Codierung gekennzeichnet oder der deaktivierte maskierte elektronische Münzdatensatz kann zerstört und/ oder gelöscht werden. Selbstverständlich kann der deaktivierte maskierte elektronische Münzdatensatz auch physisch vom Endgerät entfernt werden.

- 5 Durch das erfindungsgemäße Verfahren werden verschiedene Verarbeitungsoperationen für die elektronischen Münzdatensätze und die entsprechenden maskierten elektronischen Münzdatensätze ermöglicht. Jeder der Verarbeitungsoperationen (insbesondere das Erstellen, Deaktivieren, Aufteilen, Verbinden und Umschalten) wird dabei in der Überwachungsinstanz registriert und dort in unveränderlicher Form an die Liste der vorherigen Verarbeitungsoperationen
- 10 für den jeweiligen maskierten elektronischen Münzdatensatz angehängt. Die Registrierung ist dabei vom Bezahlvorgang zwischen den Endgeräten sowohl zeitlich als auch örtlich (räumlich) unabhängig. Die Verarbeitungsoperationen „Erstellen“ und „Deaktivieren“, die die Existenz des monetären Betrags an sich betreffen, also die Schaffung und die Vernichtung bis hin der Zerstörung von Geld bedeuten, bedürfen einer zusätzlichen Genehmigung, beispielsweise in Form
- 15 einer Signatur, durch die Herausgeberinstanz, um in der Überwachungsinstanz registriert (also protokolliert) zu werden. Die übrigen Verarbeitungsoperationen (Aufteilen, Verbinden, Umschalten) bedürfen keiner Autorisierung durch die Herausgeberinstanz oder durch den Befehlsinitiator (= Zahler, bspw. das erste Endgerät).
- 20 Eine Verarbeitung in der Direkttransaktionsschicht betrifft nur die Besitzverhältnisse und/ oder die Zuordnung der Münzdatensätze zu Endgeräten der jeweiligen elektronischen Münzdatensätze. Eine Registrierung der jeweiligen Verarbeitung in der Überwachungsinstanz wird beispielsweise durch entsprechende Listeneinträge in einer Datenbank realisiert, die eine Reihe von Markierungen umfasst, die von der Überwachungsinstanz durchgeführt werden müssen. Eine
- 25 mögliche Struktur für einen Listeneintrag umfasst beispielsweise Spalte(n) für einen Vorgänger-Münzdatensatz, Spalte(n) für einen Nachfolger-Münzdatensatz, eine Signatur-Spalte für die Herausgeberinstanz, eine Signatur-Spalte für Münzteilungsvorgänge und zumindest eine Markierungsspalte. Eine Änderung des Status der Markierung bedarf der Genehmigung durch die Überwachungsinstanz und muss sodann unveränderlich gespeichert werden. Eine Änderung ist
- 30 endgültig, wenn und nur wenn die erforderlichen Markierungen durch die Überwachungsinstanz validiert wurden, d.h. nach der entsprechenden Prüfung beispielsweise vom Status "0" in den Status "1" gewechselt wurden. Scheitert eine Prüfung oder dauert zu lang, so wird sie stattdessen beispielsweise vom Status "-" in den Status "0" gewechselt. Weitere Statuswerte sind denkbar und/oder die hier genannten Statuswerte sind austauschbar. Bevorzugt wird die Gültigkeit der
- 35 jeweiligen (maskierten) elektronischen Münzdatensätze aus den Statuswerten der Markierungen zusammengefasst jeweils in einer Spalte für jeden maskierten elektronischen Münzdatensatz, der im Registrieren der Verarbeitung involviert ist, dargestellt.

In einem weiteren Ausführungsbeispiel können wenigstens zwei vorzugsweise drei oder sogar alle der vorhergenannten Markierungen auch durch eine einzige Markierung ersetzt werden, die dann gesetzt wird, wenn alle Prüfungen erfolgreich abgeschlossen wurden. Des Weiteren lassen sich die je zwei Spalten für Vorgänger-Datensätze und Nachfolger-Datensätze zu jeweils einem zusammenfassen, in welchem alle Münzdatensätze gemeinsam aufgelistet sind. Dadurch könnten dann auch mehr als zwei elektronische Münzdatensätze je Feldeintrag verwaltet werden, und somit z.B. eine Aufspaltung in mehr als zwei Münzen realisiert werden.

Die Prüfungen durch die Überwachungsinstanz, um zu prüfen, ob eine Verarbeitung endgültig ist sind bereits oben beschrieben und sind insbesondere:

- Sind die maskierten elektronischen Münzdatensätze der Vorgänger-Spalte(n) gültig?
- Ergibt eine Überwachung den korrekten Prüfwert?
- Sind die Bereichsnachweise für die maskierten elektronischen Münzdatensätze erfolgreich?
- Ist die Signatur des maskierten elektronischen Münzdatensatzes eine gültige Signatur der Herausgeberinstanz?

Bevorzugt gilt zudem, dass ein maskierter elektronischer Münzdatensatz ungültig ist, wenn einer der folgenden Prüfungen zutrifft, also wenn:

- (1) der maskierte elektronische Münzdatensatz nicht in der Überwachungsinstanz registriert ist;
- (2) die letzte Verarbeitung des maskierten elektronischen Münzdatensatzes angibt, dass es für ihn Vorgänger-Münzdatensätze gibt, diese letzte Verarbeitung aber nicht endgültig ist; oder
- (3) die letzte Verarbeitung des maskierten elektronischen Münzdatensatzes angibt, dass es für ihn Nachfolger-Münzdatensätze gibt und diese letzte Verarbeitung endgültig ist;
- (4) der maskierte elektronische Münzdatensatz nicht der Nachfolger von einem gültigen maskierten elektronischen Datensatz ist, es sei denn er ist von der Herausgeberinstanz signiert

In einem Aspekt der Erfindung ist ein Bezahlungssystem zum Austausch von monetären Beträgen vorgesehen mit einer Überwachungsschicht mit einer Datenbank in der maskierte elektronische Münzdatensätze abgelegt sind; und einer Direkttransaktionsschicht mit zumindest zwei Endgeräten, in welche das vorhergehend beschriebene Verfahren durchführbar ist; und/oder eine Herausgeberinstanz zum Erzeugen eines elektronischen Münzdatensatzes. Dabei kann die Herausgeberinstanz nachweisen, dass der maskierte erzeugte elektronische Münzdatensatz von ihr erzeugt wurde, bevorzugt kann sich die Herausgeberinstanz durch das Signieren ausweisen und die Überwachungsinstanz kann die Signatur der Herausgeberinstanz prüfen.

In einer bevorzugten Ausgestaltung umfasst das Bezahlungssystem eine Herausgeberinstanz zum Erzeugen eines elektronischen Münzdatensatzes. Dabei kann die Herausgeberinstanz nachweisen,

dass der maskierte erzeugte elektronische Münzdatensatz von ihr erzeugt wurde, bevorzugt kann sich die Herausgeberinstanz durch das Signieren ausweisen und die Überwachungsinstanz kann die Signatur der Herausgeberinstanz prüfen.

- 5 Bevorzugt ist das Bezahlungssystem zum Durchführen des oben genannten Verfahrens und/ oder wenigstens einer der Ausführungsvarianten ausgebildet.

Ein weiterer Aspekt der Erfindung betrifft ein Währungssystem umfassend eine Herausgeberinstanz, eine Überwachungsinstanz, ein erstes Endgerät und ein zweites Endgerät, wobei die Herausgeberinstanz ausgebildet ist, einen elektronischen Münzdatensatzes zu erstellen. Der maskierte elektronische Münzdatensatz ist ausgebildet, nachweisbar durch die Herausgeberinstanz erstellt zu sein. Die Überwachungsinstanz ist zum Ausführen eines Registrierschritts wie in dem oben genannten Verfahren ausgeführt, ausgebildet Vorzugsweise sind die Endgeräte, d.h. wenigstens das erste und zweite Endgerät zum Ausführen eines des oben genannten Verfahrens zum Übertragen geeignet.

In einer bevorzugten Ausführung des Währungssystems ist lediglich die Herausgeberinstanz berechtigt, einen elektronischen Münzdatensatz initial zu erstellen. Eine Verarbeitung, beispielsweise der Schritt des Verbindens, des Aufteilens und/ oder des Umschaltens, kann und wird vorzugsweise durch ein Endgerät durchgeführt. Der Verarbeitungsschritt des Deaktivierens kann vorzugsweise nur von der Herausgeberinstanz ausgeführt werden. Somit wäre lediglich die Herausgeberinstanz berechtigt, den elektronischen Münzdatensatzes und/ oder den maskierten elektronischen Münzdatensatz zu invalidieren.

- 25 Bevorzugt sind die Überwachungsinstanz und die Herausgeberinstanz in einer Serverinstanz angeordnet oder liegen als Computerprogrammprodukt auf einem Server und/ oder einem Computer vor.

Ein elektronischer Münzdatensatz kann dabei in einer Vielzahl von unterschiedlichen Erscheinungsformen vorliegen und damit über verschiedene Kommunikationskanäle, nachfolgend auch Schnittstellen genannt, ausgetauscht werden. Ein sehr flexibler Austausch von elektronischen Münzdatensätzen ist damit geschaffen.

Der elektronische Münzdatensatz ist beispielsweise in Form einer Datei darstellbar. Eine Datei besteht dabei aus inhaltlich zusammengehörigen Daten, die auf einem Datenträger, Datenspeicher oder Speichermedium gespeichert sind. Jede Datei ist zunächst eine eindimensionale Aneinanderreihung von Bits, die normalerweise in Byte-Blöcken zusammengefasst interpretiert werden. Ein Anwendungsprogramm (Applikation) oder ein Betriebssystem selbst interpretieren diese Bit- oder Bytefolge beispielsweise als einen Text, ein Bild oder eine Tonaufzeichnung. Das

dabei verwendete Dateiformat kann unterschiedlich sein, beispielsweise kann es eine reine Textdatei sein, die den elektronischen Münzdatensatz repräsentiert. Dabei werden insbesondere der monetäre Betrag und die blinde Signatur als Datei abgebildet.

- 5 Der elektronische Münzdatensatz ist beispielsweise eine Folge von American Standard Code for Information Interchange, kurz ASCII, Zeichen. Dabei werden insbesondere der monetäre Betrag und die blinde Signatur als diese Folge abgebildet.

10 Der elektronische Münzdatensatz kann in einem Gerät auch von einer Darstellungsform in eine andere Darstellungsform umgewandelt werden. So kann beispielsweise der elektronische Münzdatensatz als QR-Code im Gerät empfangen werden und als Datei oder Zeichenfolge vom Gerät ausgegeben werden.

15 Diese unterschiedlichen Darstellungsformen von ein und demselben elektronischen Münzdatensatz ermöglichen einen sehr flexiblen Austausch zwischen Geräten unterschiedlicher technischer Ausrüstung unter Verwendung unterschiedlicher Übertragungsmedien (Luft, Papier, drahtgebunden) und unter Berücksichtigung der technischen Ausgestaltung eines Geräts. Die Wahl der Darstellungsform der elektronischen Münzdatensätze erfolgt bevorzugt automatisch, beispielsweise aufgrund erkannter oder ausgehandelter Übertragungsmedien und
20 Gerätekomponenten. Zusätzlich kann auch ein Benutzer eines Gerät die Darstellungsform zum Austausch (=Übertragen) eines elektronischen Münzdatensatzes wählen.

In einem Aspekt der Erfindung wird die Aufgabe durch ein Gerät gelöst, das zum direkten Übertragen von elektronischen Münzdatensätzen an ein anderes Gerät eingerichtet ist. Das Gerät
25 umfasst Mittel zum Zugreifen auf einen Datenspeicher, wobei im Datenspeicher zumindest ein elektronischer Münzdatensatz abgelegt ist; eine Schnittstelle zumindest zum Ausgeben des zumindest einen elektronischen Münzdatensatzes an das andere Gerät; und eine Recheneinheit, die zum Maskieren des elektronischen Münzdatensatzes im Gerät durch Anwenden der beispielsweise homomorphen (Verschlüsselungs-)Einwegfunktion auf den elektronischen
30 Münzdatensatz zum Erhalten eines maskierten elektronischen Münzdatensatzes zum Registrieren des maskierten elektronischen Münzdatensatzes in einer Überwachungsinstanz; und zum Ausgeben des elektronischen Münzdatensatzes mittels der Schnittstelle eingerichtet ist.

Ein Gerät ist dabei ein zuvor beschriebenes Endgerät bzw. eine zuvor beschriebene Maschine.

35 In einem einfachen Fall ist der Datenspeicher ein interner Datenspeicher des Geräts. Hier werden die elektronischen Münzdatensätze abgelegt. Ein einfacher Zugriff auf elektronische Münzdatensätze ist somit gewährleistet.

Der Datenspeicher ist insbesondere ein externer Datenspeicher, auch Online-Speicher genannt. Somit weist das Gerät nur ein Zugriffsmittel auf die extern und damit sicher abgelegten Münzdatensätze auf. Insbesondere bei einem Verlust des Geräts oder bei Fehlfunktionen des Geräts sind die elektronischen Münzdatensätze nicht verloren. Da der Besitz der (unmaskierten) elektronischen Münzdatensätze gleich dem Besitz des monetären Betrags entspricht, kann durch Verwendung externer Datenspeicher Geld sicherer aufbewahrt werden.

Ist die Überwachungsinstanz eine entfernte Überwachungsinstanz, so verfügt das Gerät bevorzugt über eine Schnittstelle zur Kommunikation mittels einem üblichen Internet-Kommunikationsprotokoll, beispielsweise TCP, IP, UDP oder HTTP. Die Übertragung kann eine Kommunikation über das Mobilfunknetz beinhalten.

In einer bevorzugten Ausgestaltung ist das Gerät dazu eingerichtet, die bereits beschriebenen Verarbeitungen, insbesondere das Aufteilen, Verbinden und Umschalten an einem elektronischen Münzdatensatz durchzuführen. Dazu ist die Recheneinheit dazu eingerichtet, einen umzuschaltenden elektronischen Münzdatensatz als den elektronischen Münzdatensatz zu maskieren, den die Überwachungsinstanz als maskierten elektronischen Münzdatensatz zum Registrieren des Umschalten-Befehls bzw. im Umschalten-Schritt braucht. Auf diese Weise kann ein elektronischer Münzdatensatz – wie oben beschrieben – umgeschaltet werden.

Zudem oder alternativ ist die Recheneinheit bevorzugt eingerichtet, einen in eine Anzahl von Münzteildatensätzen aufgeteilten elektronischen Münzdatensatz zu maskieren, um einen maskierten elektronischen Münzdatensatz und ggf. maskierte elektronischen Münzteildatensätze zu erhalten, die in der Überwachungsinstanz registriert werden können. Auf diese Weise kann ein elektronischer Münzdatensatz – wie oben beschrieben – aufgeteilt werden.

Zudem oder alternativ ist die Recheneinheit bevorzugt eingerichtet, einen aus einem ersten und einem zweiten elektronischen Münzdatensatz zu verbindenden elektronischen Münzteildatensatzes als den elektronischen Münzdatensatz zu maskieren, um einen maskierten verbindenden Münzdatensatzes als den maskierten elektronischen Münzdatensatz zu erhalten, der in der Überwachungsinstanz registriert wird. Auf diese Weise kann ein elektronischer Münzdatensatz – wie oben beschrieben – verbunden werden.

In einer bevorzugten Ausgestaltung ist die Schnittstelle zum Ausgeben des zumindest einen elektronischen Münzdatensatzes eine elektronische Anzeigeeinheit des Geräts, die zum Anzeigen des elektronischen Münzdatensatzes und dadurch (auch) zum Ausgeben des elektronischen Münzdatensatzes in visueller Form eingerichtet ist. Wie bereits beschrieben wurde, ist der elektronische Münzdatensatz dann beispielsweise in Form eines optoelektronisch erfassbaren Codes, einem Bild, etc. zwischen Geräten austauschbar.

In einer bevorzugten Ausgestaltung ist die Schnittstelle zum Ausgeben des zumindest einen elektronischen Münzdatensatzes eine Protokollschnittstelle zum drahtlosen Senden des elektronischen Münzdatensatzes an das andere Gerät mittels eines Kommunikationsprotokolls für Drahtloskommunikation. Dabei ist insbesondere eine Nahfeldkommunikation, beispielsweise mittels Bluetooth-Protokoll oder NFC-Protokoll oder IR-Protokoll vorgesehen, alternativ oder zusätzlich sind WLAN-Verbindungen oder Mobilfunkverbindungen denkbar. Der elektronische Münzdatensatz wird dann gemäß den Protokolleigenschaften angepasst und übertragen.

In einer bevorzugten Ausgestaltung ist die Schnittstelle zum Ausgeben des zumindest einen elektronischen Münzdatensatzes eine Datenschnittstelle zum Bereitstellen des elektronischen Münzdatensatzes an das andere Gerät mittels einer Applikation. Im Unterschied zur Protokollschnittstelle wird hier der elektronische Münzdatensatz mittels einer Applikation übertragen. Diese Applikation überträgt sodann den Münzdatensatz in einem entsprechenden Dateiformat. Es kann ein für elektronische Münzdatensätze spezifisches Dateiformat verwendet werden. In einfachster Form wird der Münzdatensatz als ASCII-Zeichenfolge oder als Textnachricht, beispielsweise SMS, MMS, Instant-Messenger-Nachricht (wie Threema oder WhatsApp) übertragen. In einer alternativen Form wird der Münzdatensatz als APDU-Zeichenfolge übertragen. Es kann auch eine Geldbörsen-Applikation vorgesehen sein. Hierbei stellen die austauschenden Geräte bevorzugt sicher, dass ein Austausch mittels der Applikation möglich ist, also dass beide Geräte die Applikation aufweisen und austauschbereit sind.

In einer bevorzugten Ausgestaltung weist das Gerät weiter eine Schnittstelle zum Empfangen von elektronischen Münzdatensätzen auf.

In einer bevorzugten Ausgestaltung ist die Schnittstelle zum Empfangen des zumindest einen elektronischen Münzdatensatzes ein elektronisches Erfassungsmodul des Geräts, eingerichtet zum Erfassen eines, in visueller Form dargestellten elektronischen Münzdatensatzes. Das Erfassungsmodul ist dann beispielsweise eine Kamera oder ein Barcode bzw. QR-Code Scanner.

In einer bevorzugten Ausgestaltung ist die Schnittstelle zum Empfangen des zumindest einen elektronischen Münzdatensatzes eine Protokollschnittstelle zum drahtlosen Empfangen des elektronischen Münzdatensatzes von einem anderen Gerät mittels eines Kommunikationsprotokolls für Drahtloskommunikation. Dabei ist insbesondere eine Nahfeldkommunikation, beispielsweise mittels Bluetooth-Protokoll oder NFC-Protokoll oder IR-Protokoll, vorgesehen. Alternativ oder zusätzlich sind WLAN-Verbindungen oder Mobilfunkverbindungen denkbar.

- In einer bevorzugten Ausgestaltung ist die Schnittstelle zum Empfangen des zumindest einen elektronischen Münzdatensatzes eine Datenschnittstelle zum Empfangen des elektronischen Münzdatensatzes von dem anderen Gerät mittels einer Applikation. Diese Applikation empfängt sodann den Münzdatensatz in einem entsprechenden Dateiformat. Es kann ein für Münzdatensätze spezifisches Dateiformat verwendet werden. In einfachster Form wird der Münzdatensatz als ASCII-Zeichenfolge oder als Textnachricht, beispielsweise SMS, MMS, Threema oder WhatsApp übertragen. In einer alternativen Form wird der Münzdatensatz als APDU-Zeichenfolge übertragen. Zusätzlich kann die Übertragung mittels einer Geldbörsen-Applikation erfolgen.
- 10 In einer bevorzugten Ausgestaltung ist die Schnittstelle zum Empfangen des zumindest einen elektronischen Münzdatensatzes auch die Schnittstelle zum Ausgeben des elektronischen Münzdatensatzes, sodass eine Schnittstelle sowohl zum Senden als auch zum Empfangen des Münzdatensatzes vorgesehen ist.
- 15 In einer bevorzugten Ausgestaltung umfassend das Gerät zumindest ein Sicherheitselement-Lesegerät, eingerichtet zum Lesen eines Sicherheitselements; einen Zufallszahlengenerator; und/oder eine Kommunikationsschnittstelle zu einem Tresormodul und/ oder Bankinstitut mit zu autorisierendem Zugriff auf ein Bankkonto.
- 20 In einer bevorzugten Ausgestaltung ist der Datenspeicher ein gemeinsamer Datenspeicher, auf den zumindest noch ein anderes Gerät zugreifen kann, wobei jedes der Endgeräte eine Applikation aufweist, wobei diese Applikation zum Kommunizieren mit der Überwachungsinstanz zum entsprechenden Registrieren von elektronischen Münzteildatensätzen eingerichtet ist.
- 25 Vorgeschlagen wird hierbei also eine Lösung, die digitales Geld in Form von elektronischen Münzdatensätzen herausgibt, die an die Verwendung von konventionellen (analogen) Banknoten und/oder Münzen angelehnt ist. Das digitale Geld wird hierbei durch elektronische Münzdatensätze abgebildet. Wie bei (analogen) Banknoten werden auch diese elektronischen Münzdatensätze für alle Formen von Zahlungen, einschließlich Peer-to-Peer-Zahlungen und/oder POS-Zahlungen, verwendbar. Die Kenntnis aller Bestandteile (insbesondere monetärer Betrag und Verschleierungsbetrag) eines gültigen elektronischen Münzdatensatzes ist gleichbedeutend mit dem Besitz (Eigentum) des digitalen Geldes. Es ist daher ratsam, diese gültigen elektronischen Münzdatensätze vertraulich zu behandeln, also beispielsweise in einem Sicherheitselement/ Tresormodul eines Endgeräts aufzubewahren und dort zu verarbeiten. Um über die Authentizität eines elektronischen Münzdatensatzes zu entscheiden und Doppelausgaben zu verhindern, werden in der Überwachungsinstanz maskierte elektronische Münzdatensätze als einzigartige, korrespondierende öffentliche Darstellung des elektronischen Münzdatensatzes vorgehalten. Die Kenntnis oder der Besitz eines maskierten elektronischen Münzdatensatzes stellt nicht den Besitz von Geld dar. Vielmehr gleicht dies dem Überprüfen der Echtheit des analogen Zahlungsmittels.
- 30
- 35

Die Überwachungsinstanz enthält auch Markierungen über durchgeführte und geplante Verarbeitungen des maskierten elektronischen Münzdatensatzes. Aus den Markierungen zu den Verarbeitungen wird ein Status des jeweiligen maskierten elektronischen Münzdatensatzes abgeleitet, der angibt, ob der entsprechende (unmaskierte) elektronische Münzdatensatz gültig, d.h. zahlungsbereit ist. Daher wird ein Empfänger eines elektronischen Münzdatensatzes zunächst einen maskierten elektronischen Münzdatensatz erzeugen und sich durch die Überwachungsinstanz die Gültigkeit der maskierten elektronischen Münzdatensatz authentifizieren lassen. Ein großer Vorteil dieser erfindungsgemäßen Lösung ist, dass das digitale Geld auf Endgeräte, Händler, Banken und andere Nutzer des Systems verteilt wird, aber kein digitales Geld oder weitere Metadaten bei der Überwachungsinstanz - also einer gemeinsamen Instanz - gespeichert wird.

Die vorgeschlagene Lösung kann in bestehende Zahlssysteme und Infrastrukturen eingebunden werden. Insbesondere können eine Kombination aus analogen Zahlungsvorgängen mit Geldscheinen und Münzen und digitale Zahlungsvorgänge gemäß der vorliegenden Lösung vorliegen. So kann ein Bezahlvorgang mit Banknoten und/ oder Münzen erfolgen, das Wechselgeld bzw. Rückgeld liegt aber als elektronischer Münzdatensatz vor. Zur Transaktion können beispielsweise ATMs mit entsprechender Konfiguration, insbesondere mit geeigneter Kommunikationsschnittstelle, und/ oder mobile Endgeräte vorgesehen sein. Weiterhin ist ein Umtausch von elektronischem Münzdatensatz in Banknoten bzw. Münzen denkbar.

Die vorliegend aufgeführten Schritte des Erstellens, Umschaltens, Aufteilens, Verbindens und Deaktivierens werden jeweils durch einen entsprechenden Erstell-, Umschalt-, Aufteil-, Verbinden- bzw. Deaktivier-Befehl ausgelöst.

Die Aufgabe wird zudem durch eine Überwachungseinheit gelöst, die eingerichtet ist zum Empfangen eines maskierten elektronischen Münzdatensatzes und zum Registrieren des maskierten elektronischen Münzdatensatzes. Der maskierte elektronische Münzdatensatz ist in einem ersten Maskierungsmodus oder einem zweiten Maskierungsmodus oder einem dritten Maskierungsmodus maskiert. Bevorzugt ist der maskierte elektronische Münzdatensatz gemäß einem Maskierungsschritt aus dem vorhergehend beschriebenen Verfahren maskiert. Die Überwachungseinheit ist zudem eingerichtet zum Registrieren eines Modifizierens eines Münzdatensatzes gemäß dem vorhergehend beschriebenen Verfahren.

KURZE ZUSAMMENFASSUNG DER FIGUREN

Nachfolgend wird anhand von Figuren die Erfindung bzw. weitere Ausführungsformen und Vorteile der Erfindung näher erläutert, wobei die Figuren lediglich Ausführungsbeispiele der Erfindung beschreiben. Gleiche Bestandteile in den Figuren werden mit gleichen Bezugszeichen

versehen. Die Figuren sind nicht als maßstabsgetreu anzusehen, es können einzelne Elemente der Figuren übertrieben groß bzw. übertrieben vereinfacht dargestellt sein.

Es zeigen:

- 5
- Fig. 1 ein Ausführungsbeispiel eines Bezahlungssystems gemäß der Erfindung;
- Fig. 2 ein Ausführungsbeispiel einer Überwachungsinstanz;
- 10 Fig. 3 ein Ausführungsbeispiel eines Bezahlungssystems gemäß der Erfindung zum Aufteilen und Umschalten von elektronischen Münzdatensätzen;
- Fig. 4 ein Ausführungsbeispiel eines Bezahlungssystems gemäß der Erfindung zum Verbinden von elektronischen Münzdatensätzen;
- 15
- Fig. 5 ein Ausführungsbeispiel eines Verfahrensablaufdiagramms eines erfindungsgemäßen Verfahrens und entsprechenden Verarbeitungsschritte eines Münzdatensatzes;
- 20
- Fig. 6 ein Ausführungsbeispiel eines Verfahrensablaufdiagramms eines erfindungsgemäßen Verfahrens und entsprechenden Verarbeitungsschritte eines Münzdatensatzes;
- Fig. 7 ein weiteres Ausführungsbeispiel eines Verfahrensablaufdiagramms eines erfindungsgemäßen Verfahrens;
- 25
- Fig. 8 ein Ausführungsbeispiel eines erfindungsgemäßen Geräts;
- Fig. 9 ein weiteres Ausführungsbeispiel eines Verfahrensablaufdiagramms eines erfindungsgemäßen Verfahrens gemäß einem vierten Maskierungsmodus;
- 30
- Fig. 10 eine schematische Darstellung des Verfahrens gemäß Fig. 9;
- Fig. 11 ein weiteres Ausführungsbeispiel eines Verfahrensablaufdiagramms eines erfindungsgemäßen Verfahrens;
- 35
- Fig. 12 ein weiteres Ausführungsbeispiel eines erfindungsgemäßen Verfahrens; und

Fig. 13 ein Verfahrensablaufdiagramm des in Fig. 12 dargestellten erfindungsgemäßen Verfahrens.

FIGURENBESCHREIBUNG

- 5 Fig. 1 zeigt ein Ausführungsbeispiel eines Bezahlsystems mit Endgeräten M1 und M2 gemäß der Erfindung. Die Endgeräte M1 und M2 können dabei auch Geräte sein.

Dabei wird in einer Herausgeberinstanz 1, beispielsweise einer Zentralbank, ein elektronischer Münzdatensatz C_i erzeugt. Zu dem elektronischen Münzdatensatz C_i wird ein maskierter elektronische Münzdatensatz Z_i erzeugt und in einem „Verschleiertelektronischen-Datensatz-Ledger“ registriert. Als Ledger wird im Rahmen dieser Erfindung eine Liste, ein Verzeichnis, vorzugsweise eine Datenbankstruktur verstanden. Der elektronische Münzdatensatz C_i wird an ein erstes Endgerät M1 ausgegeben.

- 15 Beispielsweise wurde dazu als Verschleierungsbetrag r_i eine echte Zufallszahl erzeugt. Diese Verschleierungsbetrag r_i wird mit einem monetären Betrag v_i verknüpft und bildet sodann einen erfindungsgemäßen i-ten elektronischen Münzdatensatz:

$$C_i = \{v_i, r_i\} \quad (1)$$

- 20 Ein gültiger elektronischer Münzdatensatz kann zur Bezahlung eingesetzt werden. Der Besitzer der beiden Werte v_i und r_i ist daher im Besitz des digitalen Geldes. Das digitale Geld ist aber definiert durch ein Paar bestehend aus einem gültigen elektronischen Münzdatensatz und einem entsprechenden maskierten elektronischen Münzdatensatz Z_i . Der maskierte elektronische Münzdatensatz Z_i wird durch Anwenden einer Einwegfunktion $f(C_i)$ gemäß Gleichung (2) erhalten:

$$Z_i = f(C_i) \quad (2)$$

- Die Einwegfunktion $f(C_i)$ ist beispielsweise homomorph. Der maskierte elektronische Münzdatensatz ist beispielsweise ein vollständig elektronischer maskierter Münzdatensatz, ein quasimaskierter elektronischer Münzdatensatz oder ein teilbetragsmaskierter elektronischer Münzdatensatz, wie in Bezug auf Fig. 9 und folgende noch detailliert ausgeführt wird.

- Diese Funktion $f(C_i)$ ist insbesondere für einen vollständig maskierten elektronischen Münzdatensatz einen unvollständig maskierten elektronischen Münzdatensatz und einen teilweise maskierten elektronischen Münzdatensatz öffentlich, d.h. jeder Systemteilnehmer am Bezahlssystem kann diese Funktion aufrufen und verwenden. Diese Funktion $f(C_i)$ ist gemäß Gleichung (3) oder Gleichung (3a) beispielsweise definiert:

$$Z_i = v_i \cdot H + r_i \cdot G \quad (3)$$

$$Z_i = r_i \cdot G \quad (3a)$$

wobei H und G Generatorpunkte einer Gruppe, in der das diskrete Logarithmusproblem schwer ist, mit den Generatoren G und H, für die der diskrete Logarithmus der jeweils anderen Basis unbekannt ist. Beispielsweise ist G (Gleichung (3), (3a)) als auch H (Gleichung (3)) jeweils ein Generatorpunkt einer elliptischen Kurvenverschlüsselung, ECC, - also private Schlüssel der ECC, sind. Im Fall von Gleichung (3) müssen diese Generatorpunkte G und H in der Art gewählt werden, dass der Zusammenhang von G und H nicht öffentlich bekannt ist, sodass bei:

$$G = n \cdot H \quad (4)$$

die Verknüpfung n praktisch nicht auffindbar sein darf, um zu verhindern, dass der monetäre Betrag v_i manipuliert wird und trotzdem ein gültiges Z_i berechnet werden könnte. Die Gleichung (3) ist ein „Pederson-Commitment für ECC“, das sicherstellt, dass der monetäre Betrag v_i einer Überwachungsinstanz 2 zugestanden, also „committed“, werden kann, ohne diesen der Überwachungsinstanz 2 zu offenbaren. Der öffentlichen und entfernten Überwachungsinstanz 2 wird daher nur der maskierte Münzdatensatz Z_i zugesendet (offenbart).

Auch wenn im vorliegenden Beispiel eine Verschlüsselung basierend auf elliptischen Kurven beschrieben ist bzw. wird, so wäre auch ein anderes kryptographische Verfahren denkbar, welches auf einem diskreten logarithmischen Verfahren beruht und auf Gleichung (3a) basiert.

Bei Anwendung der Gleichung (3a) wird eine Einwegfunktion nur auf einen Teil des Münzdatensatzes C, hier der Verschleierungsbetrag r (für einen quasimaskierten Münzdatensatz) oder einen ersten monetären Betragsteil des monetären Betrags (für einen teilbetragsmaskierten Münzdatensatz), angewendet.

Der maskierte Verschleierungsbetrag kann auch als R bezeichnet werden.

Die Gleichung (3) ermöglicht durch die Entropie des Verschleierungsbetrags r_i , dass auch bei kleinem Wertebereich für monetäre Beträge v_i ein kryptografisch starkes Z_i erhalten wird. Somit ist ein einfacher Brute-Force-Angriff durch bloßes Schätzen von monetären Beträgen v_i praktisch nicht möglich.

Die Gleichungen (3) und (3a) verwenden Einwegfunktionen, das heißt, dass die Berechnung von Z_i aus C_i einfach ist, da ein effizienter Algorithmus existiert, wohingegen die Berechnung von C_i ausgehend von Z_i sehr schwer ist, da kein in polynomialer Zeit lösbarer Algorithmus existiert.

Zudem ist die Gleichung (3) homomorph für Addition und Subtraktion, das heißt es gilt:

$$Z_i + Z_j = (v_i \cdot H + r_i \cdot G) + (v_j \cdot H + r_j \cdot G) = (v_i + v_j) \cdot H + (r_i + r_j) \cdot G \quad (5)$$

5 Somit können Additions-Operationen und Subtraktions-Operationen sowohl in der Direkttransaktionsschicht 3 also auch parallel in der Überwachungsschicht 4 ausgeführt werden, ohne dass die Überwachungsschicht 4 Kenntnis von den elektronischen Münzdatensätzen C_i hat. Die homomorphe Eigenschaft der Gleichung (3) ermöglicht eine Überwachung von gültigen und ungültigen elektronischen Münzdatensätzen C_i auf alleiniger Basis der maskierten
10 Münzdatensätze Z_i zu führen und sicherzustellen, dass kein neuer monetärer Betrag v_j geschaffen wurde.

Durch diese homomorphe Eigenschaft kann der Münzdatensatz C_i gemäß Gleichung (1) aufgeteilt werden in:

$$C_i = C_j + C_k = \{v_j; r_j\} + \{v_k; r_k\} \quad (6)$$

15

wobei gilt:

$$v_i = v_j + v_k \quad (7)$$

$$r_i = r_j + r_k \quad (8)$$

Für die entsprechenden maskierten Münzdatensätze gilt:

$$Z_i = Z_j + Z_k \quad (9)$$

20

Mit Gleichung (9) kann beispielsweise auf einfache Weise eine „Aufteilen“-Verarbeitung bzw. ein „Aufteilen“-Verarbeitungsschritt eines Münzdatensatzes gemäß Fig. 3 geprüft werden, ohne dass die Überwachungsinstanz 2 Kenntnis von C_i , C_j , C_k hat. Insbesondere wird die Bedingung der Gleichung (9) geprüft, um aufgeteilte Münzdatensätze C_j und C_k für gültig zu erklären und den
25 Münzdatensatz C_i für ungültig zu erklären. Ein derartiges Aufteilen eines elektronischen Münzdatensatzes C_i ist in Fig. 3 gezeigt.

Auf die gleiche Weise können elektronische Münzdatensätze auch zusammengefügt (verbunden) werden, siehe dazu Fig. 4 und die Erläuterungen dazu.

30

Zusätzlich gilt es zu prüfen, ob (nicht erlaubte) negative monetäre Beträge registriert werden. Ein Besitzer eines elektronischen Münzdatensatzes C_i muss dabei der Überwachungsinstanz 2 nachweisen können, dass alle monetären Beträge v_i in einer Verarbeitungs-Operation innerhalb eines Wertebereichs von $[0, \dots, 2^n-1]$ liegen, ohne der Überwachungsinstanz 2 dabei die

monetären Beträge v_i mitzuteilen. Diese Bereichsnachweise werden auch „Range-Proofs“ genannt. Als Bereichsnachweise werden bevorzugt Ringsignaturen (engl. ring signature) verwendet. Für das vorliegende Ausführungsbeispiel werden sowohl der monetäre Betrag v als auch der Verschleierungsbetrag r eines elektronischen Münzdatensatzes C in Bitdarstellung aufgelöst. Es gilt:

$$v_i = \sum a_j \cdot 2^j \text{ für } 0 \leq j < n \text{ und } a_j \text{ „element“ } \{0; 1\} \quad (9a)$$

sowie

$$r_i = \sum b_j \cdot 2^j \text{ für } 0 \leq j < n \text{ und } b_j \text{ „element“ } \{0; 1\} \quad (9b)$$

Für jedes Bit wird vorzugsweise eine Ringsignatur mit

$$C_{ij} = a_j \cdot H + b_j \cdot G \quad (9c)$$

und

$$C_{ij} - a_j \cdot H \quad (9d)$$

durchgeführt, wobei in einer Ausgestaltung vorgesehen sein kann, nur für bestimmte Bits eine Ringsignatur durchzuführen.

In Fig. 1 wird ein elektronischer Münzdatensatz C_i von der Herausgeberinstanz 1 erzeugt und mittels der Gleichung (3) oder der Gleichung (3a) ein maskierter elektronischer Münzdatensatz Z_i von der Herausgeberinstanz 1 errechnet und dieser in der Überwachungsinstanz 2 registriert.

Im Anschluss überträgt das erste Endgerät M1, das den elektronischen Münzdatensatz C_i an ein zweites Endgerät M2 übertragen kann oder einen der Verarbeitungs-Schritte (Umschalten, Verbinden, Aufteilen) ausführen kann. Die Übertragung erfolgt beispielsweise drahtlos über WLAN, NFC oder Bluetooth. Die Übertragung kann durch kryptografische Verschlüsselungsverfahren zusätzlich abgesichert sein, indem beispielsweise ein Sitzungsschlüssel ausgehandelt wird oder eine PKI-Infrastruktur angewendet wird.

Im zweiten Endgerät M2 wird der übertragene elektronische Münzdatensatz C_i als C_i^* erhalten. Mit dem Erhalt des elektronischen Münzdatensatzes C_i^* ist das zweite Endgerät M2 im Besitz des digitalen Geldes, den der elektronische Münzdatensatz C_i^* repräsentiert. Wenn sich beide Endgeräte gegenseitig vertrauen, sind keine weiteren Schritte notwendig, um das Verfahren zu beenden. Allerdings ist dem Endgerät M2 nicht bekannt, ob der elektronische Münzdatensatz C_i^* tatsächlich gültig ist. Zudem könnte das Endgerät M1 den elektronischen Münzdatensatz C_i auch

noch einem dritten Endgerät (nicht dargestellt) übertragen. Um dies zu verhindern sind weitere bevorzugte Schritte im Verfahren vorgesehen.

Zum Prüfen der Validität des erhaltenen elektronischen Münzdatensatzes C_i^* wird im zweiten Endgerät M2 mit der – öffentlichen – Einwegfunktion aus Gleichung (3) oder Gleichung (3a) der maskierte übertragene elektronische Münzdatensatz Z_i^* errechnet. Der maskierte übertragene elektronische Münzdatensatz Z_i^* wird dann an die Überwachungsinstanz 2 übertragen und dort gesucht. Bei Übereinstimmung mit einem registrierten und gültigen maskierten elektronischen Münzdatensatz wird dem zweiten Endgerät M2 die Validität des erhaltenen Münzdatensatzes C_i^* angezeigt und es gilt, dass der erhaltene elektronische Münzdatensatz C_i^* gleich dem registrierten elektronischen Münzdatensatz C_i ist. Mit der Prüfung auf Validität kann in einer Ausgestaltung festgestellt werden, dass der erhaltene elektronische Münzdatensatz C_i^* noch gültig ist, d.h., dass er nicht bereits durch einen anderen Verarbeitungsschritt oder bei einer anderen Transaktion bereits verwendet wurde und/ oder einer weiteren Veränderung unterworfen war.

Bevorzugt findet danach ein Umschalten des erhaltenen elektronischen Münzdatensatzes statt.

Es gilt für das erfindungsgemäße Verfahren, dass die alleinige Kenntnis eines (vollständig, unvollständig, quasi- oder teil-) maskierten elektronischen Münzdatensatzes nicht dazu berechtigt, das digitale Geld auszugeben. Die alleinige Kenntnis des elektronischen Münzdatensatzes C_i berechtigt aber zum Bezahlen, d.h. eine Transaktion erfolgreich durchzuführen, insbesondere wenn der Münzdatensatz C_i gültig ist. Es herrscht eine eindeutige Beziehung zwischen den elektronischen Münzdatensätzen C_i und den entsprechenden maskierten elektronischen Münzdatensätzen. Die maskierten elektronischen Münzdatensätze werden in der Überwachungsinstanz 2, beispielsweise einer öffentlichen dezentralen Datenbank, registriert. Durch dieses Registrieren wird zunächst die Gültigkeit des elektronischen Münzdatensatzes C_i prüfbar, beispielsweise ob neue monetäre Beträge (illegaler Weise) erschaffen wurden.

Ein Hauptunterscheidungsmerkmal gegenüber konventionellen Lösungen ist, dass die maskierten elektronischen Münzdatensätze in einer Überwachungsschicht 4 gespeichert werden und alle Verarbeitungen an dem elektronischen Münzdatensatz dort registriert werden, wohingegen die tatsächliche Übertragung des digitalen Geldes in einer (geheimen, d.h. einer der Öffentlichkeit nicht bekannten) Direkttransaktionsschicht 3 erfolgt.

Um ein mehrfaches Ausgeben zu verhindern oder um ein flexibleres Übertragen zu gewährleisten, können die elektronischen Münzdatensätze nunmehr im erfindungsgemäßen Verfahren verarbeitet werden. In der nachfolgenden Tabelle 1 sind die einzelnen Operationen aufgelistet, wobei mit dem angegebenen Befehl auch ein entsprechender Verarbeitungsschritt ausgeführt wird:

Befehl bzw. Schritt	Signatur erstellen	Zufallszahl erstellen	Maskierung erstellen	Bereichsnachweis erstellen
Erzeugen	1	1	1	0 oder 1
Deaktivieren	1	0	1	0 oder 1
Aufteilen	0	1	3	0 oder 1
Verbinden	0	0	3	1
Umschalten	0	1	2	1

Tabelle 1 – Anzahl von Operationen, die pro Verarbeitung eines Münzdatensatzes im Endgerät bzw.

Herausgeberinstanz durchführbar sind;

Weitere Operationen, die in Tabelle 1 nicht aufgeführt sind, können benötigt werden. Anstelle der angeführten Implementierung sind auch andere Umsetzungen denkbar, die andere Operationen implizieren. Die Tabelle 1 zeigt, dass für jeden Münzdatensatz, jede der Verarbeitungen „Erstellen“, „Deaktivieren“, „Aufteilen“, „Verbinden“ und „Umschalten“ verschiedene Operationen „Signatur erstellen“, „Zufallszahl erstellen“, „Maskierung erstellen“, „Bereichsprüfung“ vorgesehen sein können, wobei jede der Verarbeitungs-Operation in der Überwachungsinstanz 2 registriert und dort in unveränderlicher Form an eine Liste vorheriger Verarbeitungs-Operationen für maskierte elektronische Münzdatensätze angehängt wird. Die Operationen der Verarbeitungen „Erstellen“ und „Deaktivieren“ eines elektronischen Münzdatensatzes werden nur an sicheren Orten und/ oder nur von ausgewählten Instanzen, beispielsweise der Herausgeberinstanz 1, ausgeführt, während die Operationen aller übrigen Verarbeitungen auf den Endgeräten M1 bis M3 ausgeführt werden können.

Die Anzahl der Operationen für die einzelnen Verarbeitungen ist in der Tabelle 1 mit „0“, „1“ oder „2“ gekennzeichnet. Die Anzahl „0“ zeigt dabei an, dass das Endgerät bzw. die Herausgeberinstanz 1 diese Operation für diese Verarbeitung des elektronischen Münzdatensatzes nicht durchführen muss. Die Anzahl „1“ zeigt dabei an, dass das Endgerät bzw. die Herausgeberinstanz 1 diese Operation für diese Verarbeitung des elektronischen Münzdatensatzes einmal durchführen können muss. Die Anzahl „2“ zeigt dabei an, dass das Endgerät bzw. die Herausgeberinstanz 1 diese Operation zweimal für diese Verarbeitung des elektronischen Münzdatensatzes durchführen können muss.

Grundsätzlich kann in einer Ausgestaltung auch vorgesehen sein, dass eine Bereichsprüfung durch die Herausgeberinstanz 1 auch beim Erzeugen und/ oder Löschen durchgeführt wird.

In der nachfolgenden Tabelle 2 sind für die einzelnen Verarbeitungen die für die Überwachungsinstanz 2 benötigten Operationen aufgelistet:

Befehl bzw. Schritt	Signatur vom Herausgeber prüfen	Gültigkeit des maskierten elektronischen	Bereichsnachweis	homomorphe Eigenschaften der maskierten elektronischen
---------------------	---------------------------------	--	------------------	--

		Münzdatensatzes prüfen	nachvoll- ziehen	Münzdatensätze nachvollziehen, d.h. Addieren oder Subtrahieren
Erzeugen	1	0	0 oder 1	0
Deaktivieren	1	1	0 oder 1	0
Aufteilen	0	1	2 oder mehr	1
Verbinden	0	2 oder mehr	1	1
Umschalten	0	1	1	0

Tabelle 2 - Anzahl von Operationen, die pro Verarbeitung eines Münzdatensatzes in der Überwachungsinstanz durchführbar sind;

Weitere Operationen, die in Tabelle 2 nicht aufgeführt sind, können benötigt werden. Anstelle der angeführten Implementierung sind andere Umsetzungen denkbar, die andere Operationen implizieren. Alle Operationen der Tabelle 2 können in der Überwachungsinstanz 2 durchgeführt werden, die als vertrauenswürdige Instanz, beispielsweise als dezentraler Server, insbesondere Distributed-Trusted-Server, für eine ausreichende Integrität der elektronischen Münzdatensätze sorgt.

Die Tabelle 3 zeigt die für die Systemteilnehmer im Bezahlssystem der Fig. 1 bevorzugt zu installierenden Komponenten:

Befehl bzw. Schritt	Herausgeber- instanz	Endgerät	Überwachungsinstanz
Zufallszahlgenerator (hohe Sicherheit)	Ja	-	-
Zufallsgenerator (deterministisch)	-	Ja	-
PKI zum Signieren	Ja	-	-
PKI zur Signaturprüfung	-	(Ja)	Ja
Lesezugriff auf Datenbank	Ja	Ja	Ja
Schreibzugriff auf Datenbank	Ja	Ja	Ja
Deaktivieren des elektronischen Münzdatensatzes	Ja	Ja	-
Transportverschlüsselung	Ja	Ja	-
Sicherer Speicher	(Ja)	Ja	-/Ja
Maskierungs-Einheit	Ja	Ja	-
Bereichsnachweis	-	Ja	-
Bereichsnachweis prüfen	-	-	Ja
Datenbank Software	-	-	Ja

Tabelle 3 – Bevorzugte Einheiten in den Systemkomponenten

Tabelle 3 zeigt eine Übersicht über die bevorzugt zu verwendenden Komponenten in jedem Systemteilnehmer, also der Herausgeberinstanz 1, einem Endgerät M1 und der Überwachungsinstanz 2. Das Endgerät M1 kann als ein Wallet für elektronische Münzdatensätze C_i , d.h. als elektronische Geldbörse, also ein Datenspeicher des Endgeräts M1, in dem eine

Vielzahl von Münzdatensätzen C_i hinterlegt sein können, ausgebildet sein und beispielsweise in Form einer Applikation auf einem Smartphone oder IT-System eines Händlers, einer Geschäftsbank oder eines anderen Marktteilnehmers implementiert sein und einen elektronischen Münzdatensatz senden oder empfangen. Somit sind die Komponenten in dem Endgerät, so wie sie in Tabelle 3 gezeigt sind, als Software implementiert. Es wird davon ausgegangen, dass die Überwachungsinstanz 2 eine Datenbank ist, die von einer Reihe vertrauenswürdiger Marktteilnehmer betrieben wird. In einer Ausgestaltung ist die Überwachungsinstanz 2 eine DLT.

Fig. 2 zeigt ein Ausführungsbeispiel einer Überwachungsinstanz 2 der Fig. 1. In der Fig. 2 ist eine beispielhafte Datenbank in Form einer Tabelle dargestellt, in der die maskierten elektronischen Münzdatensätze (hier der Einfachheit halber die vollständig maskierten elektronischen Münzdatensätze Z_i) und ggf. ihre Verarbeitungen registriert sind. Die Überwachungsinstanz 2 ist bevorzugt lokal entfernt von den Endgeräten M1 bis M3 angeordnet und ist beispielsweise in einer Server-Architektur untergebracht.

Jede Verarbeitungs-Operation für eine Verarbeitung (Erstellen, Deaktivieren, Aufteilen, Verbinden und Umschalten) wird dabei in der Überwachungsinstanz 2 registriert und dort in unveränderlicher Form an eine Liste vorheriger Verarbeitung-Operationen für maskierte elektronische Münzdatensätze angehängt. Die einzelnen Operationen bzw. deren Prüfergebnis, also quasi die Zwischenergebnisse einer Verarbeitung, werden in der Überwachungsinstanz 2 festgehalten.

Die Verarbeitungen „Erstellen“ und „Deaktivieren“, die die Existenz des monetären Betrags v_i an sich betreffen, also die Schaffung und die Vernichtung von Geld bedeuten, bedürfen einer zusätzlichen Genehmigung durch die Herausgeberinstanz 1, um in der Überwachungsinstanz 2 registriert (also protokolliert) zu werden. Die übrigen Verarbeitungsoperationen (Aufteilen, Verbinden, Umschalten) bedürfen keiner Autorisierung durch die Herausgeberinstanz 1 oder durch den Befehlsinitiator (= Zahler, bspw. das erste Endgerät M1).

Eine Registrierung der jeweiligen Verarbeitung in der Überwachungsinstanz 2 wird beispielsweise durch entsprechende Listeneinträge in der Datenbank gemäß Fig. 2 realisiert. Jeder Listeneintrag hat dabei weitere Markierungen 25 bis 28, die die Zwischenergebnisse der jeweiligen Verarbeitung dokumentiert, die von der Überwachungsinstanz 2 durchgeführt werden müssen. Bevorzugt werden die Markierungen 25 bis 28 als Hilfestellung benutzt und nach Abschluss der Befehle von der Überwachungsinstanz verworfen. Was bleibt sind Markierungen 29 bis 32 über die Gültigkeit der (maskierten) elektronischen Münzdatensätze aus den Spalten 22a, 22b, 23a und/oder 23b. Diese Markierungen sind bei eingehen eines Verarbeitung-Befehls beispielsweise im Zustand „-“ und werden nach erfolgreichem Absolvieren aller Prüfungen auf den Zustand „1“ gesetzt und bei mindestens einer gescheiterten Prüfung auf den Zustand „0“ gesetzt. Eine mögliche Struktur für

- einen Listeneintrag eines Münzdatensatzes umfasst beispielsweise zwei Spalten 22a, 22b für einen Vorgänger-Münzdatensatz (O1, O2), zwei Spalten 23a, 23b für einen Nachfolger-Münzdatensatz (S1, S2), eine Signatur-Spalte 24 für Herausgeberinstanz(en) 1, und vier Markierungsspalten 25 bis 28. Jeder der Einträge in den Spalten 25 bis 28 weist drei alternative Zustände „-“, „1“ oder „0“ auf. Die Spalte 25 (O-Flag) zeigt an, ob eine Gültigkeitsprüfung bezüglich eines elektronischen Münzdatensatzes in Spalte 22a/b erfolgreich war, wobei Zustand „1“ bedeutet, dass eine Validitäts-Prüfung ergab, dass der elektronische Münzdatensatz der Spalte 22a/b gültig ist und der Zustand „0“ anzeigt, dass eine Validitäts-Prüfung ergab, dass der elektronische Münzdatensatz der Spalte 22a/b ungültig und der Zustand „-“ anzeigt, dass eine Validitäts-Prüfung noch nicht abgeschlossen ist. Die Spalte 26 (C-Flag) zeigt an, ob die Berechnung des maskierten elektronischen Münzdatensatzes erfolgreich war, wobei Zustand „1“ bedeutet, dass eine Berechnung erfolgreich war und der Zustand „0“ gibt an, dass Berechnung nicht erfolgreich war und der Zustand „-“ anzeigt, dass eine Validitäts-Prüfung noch nicht abgeschlossen ist.
- Die in Spalte 26 durchzuführende Berechnung für vollständig maskierte Münzdatensätze basierend auf Gleichung (3) lautet beispielsweise:

$$(Z_{O1} + Z_{O2}) - (Z_{S1} + Z_{S2}) == 0 \quad (10)$$

- Die Spalte 27 (R-Flag) zeigt an, ob eine Prüfung der Bereichsnachweise oder des Bereichsnachweises erfolgreich war, wobei Zustand „1“ bedeutet, dass eine Validitäts-Prüfung ergab, dass die Bereichsnachweise oder der Bereichsnachweis nachzuvollziehen sind oder ist und der Zustand „0“ anzeigt, dass eine Validitäts-Prüfung ergab, dass die Bereichsnachweise oder der Bereichsnachweis nicht nachvollzogen werden konnten oder konnte und der Zustand „-“ anzeigt, dass eine Validitäts-Prüfung noch nicht abgeschlossen ist, erfolgreich war.

- Die Spalte 28 (S-Flag) zeigt an, ob eine Signatur des elektronischen Münzdatensatzes mit der Signatur der Spalte 24 übereinstimmt, wobei Zustand „1“ bedeutet, dass eine Validitäts-Prüfung ergab, dass die Signatur als die der Herausgeberinstanz identifiziert werden konnte und der Zustand „0“ anzeigt, dass eine Validitäts-Prüfung ergab, dass die Signatur nicht als die der Herausgeberinstanz identifiziert werden konnte und der Zustand „-“ anzeigt, dass eine Validitäts-Prüfung noch nicht abgeschlossen ist.

- Eine Änderung des Status eines der Markierungen (auch als „Flag“ bezeichnet) bedarf der Genehmigung durch die Überwachungsinstanz 2 und muss sodann unveränderlich in der Überwachungsinstanz 2 gespeichert werden. Eine Verarbeitung ist endgültig, wenn und nur wenn die erforderlichen Markierungen 25 bis 28 durch die Überwachungsinstanz 2 validiert wurden, d.h. nach der entsprechenden Prüfung vom Zustand „0“ in den Zustand „1“ oder den Zustand „1“ gewechselt wurden.

Um festzustellen, ob ein maskierter elektronischer Münzdatensatz gültig ist, sucht die Überwachungsinstanz 2 nach der letzten Änderung, die den maskierten elektronischen Münzdatensatz betrifft. Es gilt, dass der maskierte elektronische Münzdatensatz gültig ist, wenn und nur wenn der maskierte elektronische Münzdatensatz für seine letzte Verarbeitung in einer der Nachfolger-Spalten 23a, 23b aufgeführt ist und diese letzte Verarbeitung die entsprechende endgültige Markierung 25 bis 28 aufweist. Es gilt auch, dass der maskierte elektronische Münzdatensatz gültig ist, wenn und nur wenn der maskierte elektronische Münzdatensatz für seine letzte Verarbeitung in einer der Vorgänger-Spalten 22a, 22b aufgeführt ist und diese letzte Verarbeitung fehlgeschlagen ist, also zumindest einer der entsprechend geforderten Zustände der Markierungen 25 bis 28 auf „0“ gesetzt ist.

Es gilt zudem, dass der maskierte elektronische Münzdatensatz für alle übrigen Fälle nicht gültig ist, beispielsweise, wenn der maskierte elektronische Münzdatensatz nicht in der Überwachungsinstanz 2 gefunden wird oder wenn die letzte Verarbeitung des maskierten elektronischen Münzdatensatzes in einer der Nachfolger-Spalten 23a, 23b aufgeführt ist, diese letzte Verarbeitung aber nie endgültig wurde oder wenn die letzte Verarbeitung des maskierten elektronischen Münzdatensatzes in einer der Vorgänger-Spalten 22a, 22b ist und diese letzte Verarbeitung endgültig ist.

Die Prüfungen durch die Überwachungsinstanz 2, um zu prüfen, ob eine Verarbeitung endgültig ist, werden durch die Spalten 25 bis 28 abgebildet: Der Zustand in der Spalte 25 zeigt an, ob der/die maskierten elektronischen Münzdatensätze gemäß Vorgänger-Spalten 22a, 22b gültig sind. Der Zustand in der Spalte 26 gibt an, ob die Berechnung des maskierten elektronischen Münzdatensatzes gemäß Gleichung (10) stimmt. Der Zustand in der Spalte 27 gibt an, ob die Bereichsnachweise für die maskierten elektronischen Münzdatensätze erfolgreich geprüft werden konnten. Der Zustand in Spalte 28 zeigt an, ob die Signatur in der Spalte 24 des maskierten elektronischen Münzdatensatzes eine gültige Signatur der Herausgeberinstanz 1 ist.

Der Zustand „0“ in einer Spalte 25 bis 28 zeigt dabei an, dass die Prüfung nicht erfolgreich war. Der Zustand „1“ in einer Spalte 25 bis 28 zeigt dabei an, dass die Prüfung erfolgreich war. Der Zustand „-“ in einer Spalte 25 bis 28 zeigt dabei an, dass keine Prüfung erfolgt ist. Die Zustände können auch einen anderen Wert aufweisen, solange eindeutig zwischen Erfolg/Misserfolg einer Prüfung unterschieden werden kann und ersichtlich ist, ob eine bestimmte Prüfung durchgeführt wurde.

Beispielhaft sind fünf verschiedene Verarbeitungen definiert, die hier im Einzelnen erläutert werden. Dabei wird auf den entsprechenden Listeneintrag in Fig. 2 verwiesen.

Eine Verarbeitung ist beispielsweise „Erzeugen“ eines elektronischen Münzdatensatzes C_i . Das Erzeugen in der Direkttransaktionsschicht 3 durch die Herausgeberinstanz 1 beinhaltet das Wählen eines monetären Betrags v_i und das Erstellen eines Verschleierungsbetrags r_i , wie mit Gleichung (1) bereits beschrieben wurde. Wie in Fig. 2 gezeigt, bedarf es bei der Verarbeitung „Erzeugen“
5 keiner Eintragungen/Markierungen in den Spalten 22a, 22b, 23b und 25 bis 27. In der Nachfolger-Spalte 23a wird der maskierte elektronische Münzdatensatz Z_i registriert. Diese Registrierung erfolgt bevorzugt vor dem Übertragen an ein Endgerät M1 bis M3, insbesondere oder bereits beim Generieren durch die Herausgeberinstanz 1, wobei in beiden Fällen dazu die Gleichung (3) oder die Gleichung (3a) ausgeführt werden muss. Der maskierte elektronische Münzdatensatz Z_i ist
10 beim Erstellen von der Herausgeberinstanz 1 signiert, diese Signatur ist in der Spalte 24 eingetragen, um sicherzustellen, dass der elektronische Münzdatensatz C_i tatsächlich von einer Herausgeberinstanz 1 erstellt wurde, wobei auch andere Verfahren dafür in Frage kommen. Stimmt die Signatur eines erhaltenen Z_i mit der Signatur in Spalte 24 überein, so wird die Markierung in Spalte 28 gesetzt (von „0“ auf „1“). Die Markierungen gemäß Spalte 25 bis 27
15 benötigen keine Statusänderung und können ignoriert werden. Der Bereichsnachweis wird nicht benötigt, da die Überwachungsinstanz 2 darauf vertraut, dass die Herausgeberinstanz 1 keine negativen monetären Beträge ausgibt. In einer alternativen Ausführung kann er aber von der Herausgeberinstanz 1 im Erstellen-Befehl mitgesendet werden und von der Überwachungsinstanz 2 geprüft werden.

20 Eine Verarbeitung ist beispielsweise „Deaktivieren“. Das Deaktivieren, also das Geldvernichten (DESTROY), bewirkt, dass der maskierte elektronische Münzdatensatz Z_i nach erfolgreichem Ausführen des Deaktivieren-Befehls durch die Herausgeberinstanz 1 ungültig wird. Man kann also den zu deaktivierenden (maskierten) elektronischen Münzdatensatz in der Überwachungsschicht
25 4 also nicht mehr weiterverarbeiten. Um Verwirrung zu vermeiden, sollten die entsprechenden (unmaskierten) elektronischen Münzdatensätze C_i auch in der Direkttransaktionsschicht 3 deaktiviert werden. Beim „Deaktivieren“ wird die Vorgängerspalte 22a mit dem elektronischen Münzdatensatz Z_i beschrieben, aber keine Nachfolgerspalte 23a, 23b besetzt. Der maskierte elektronische Münzdatensatz Z_i ist beim Deaktivieren daraufhin zu prüfen, ob die Signatur mit der
30 Signatur gemäß Spalte 24 übereinstimmt, um sicherzustellen, dass der elektronische Münzdatensatz C_i tatsächlich von einer Herausgeberinstanz 1 erstellt wurde, wobei wieder andere Mittel für diese Prüfung verwendet werden können. Kann das signierte Z_i , das im Deaktivieren-Befehl mitgesendet wird, als von der Herausgeberinstanz 1 signiert bestätigt werden oder als gültig signiert bestätigt werden, wird die Markierung 28 gesetzt (von „0“ auf „1“). Die Markierungen
35 gemäß Spalte 26 bis 27 benötigen keine Statusänderung und können ignoriert werden. Die Markierungen gemäß Spalte 25 und 28 werden nach entsprechender Prüfung gesetzt.

Eine Verarbeitung ist beispielsweise das „Aufteilen“. Das Aufteilen, also das Teilen eines elektronischen Münzdatensatzes Z_i in eine Anzahl n , beispielsweise 2, von elektronischen

Münzteildatensätzen Z_j und Z_k erfolgt zunächst in der Direkttransaktionsschicht 3, so wie es in Fig. 3, 5 bis 7 und auch Fig. 9 bis 11 noch gezeigt wird, wobei die monetären Beträge v_j und des Verschleierungsbetrags r_j generiert werden. v_k und r_k ergeben sich durch Gleichungen (7) und (8). In der Überwachungsinstanz 2 werden die Markierungen 25 bis 27 gesetzt, die Vorgängerspalte 22a wird mit dem elektronischen Münzdatensatz Z_i beschrieben, Nachfolgerspalte 23a wird mit Z_j und Nachfolgerspalte 23b wird mit Z_k beschrieben. Die gemäß Spalten 25 bis 27 benötigten Statusänderungen erfolgen nach der entsprechenden Prüfung durch die Überwachungsinstanz 2 und dokumentieren das jeweilige Prüfungsergebnis. Die Markierung gemäß Spalte 28 wird ignoriert. In der Spalte 24 kann eine Signatur des aufgeteilten – mit Gleichung (3a) maskierten - Münzdatensatzes eingetragen werden.

Eine Verarbeitung ist beispielsweise „Verbinden“. Das Verbinden, also das Zusammenfügen zweier elektronischer Münzdatensätze Z_i und Z_j zu einem elektronischen Münzdatensatz Z_m erfolgt zunächst in der Direkttransaktionsschicht 3, so wie es in Fig. 4 noch gezeigt wird, wobei der monetäre Betrag v_m und der Verschleierungsbetrag r_m berechnet werden. In der Überwachungsinstanz 2 werden die Markierungen 25 bis 27 gesetzt, die Vorgängerspalte 22a wird mit dem elektronischen Münzdatensatz Z_i beschrieben, Vorgängerspalte 22b wird mit Z_j und Nachfolgerspalte 23b wird mit Z_m beschrieben. Die Markierungen in den Spalten 25 bis 27 benötigen Statusänderungen und die Überwachungsinstanz 2 führt die entsprechenden Prüfungen durch. Ein Bereichsnachweis muss erbracht werden, um zu zeigen, dass kein neues Geld generiert wurde. Die Markierung gemäß Spalte 28 wird ignoriert. In der Spalte 24 kann eine erste Signatur und eine zweite Signatur der zu verbindenden – mit Gleichung (3a) maskierten - Münzdatensätze eingetragen werden.

Eine Verarbeitung ist beispielsweise „Umschalten“. Das Umschalten ist dann nötig, wenn ein elektronischer Münzdatensatz auf ein anderes Endgerät übertragen wurde und ein erneutes Ausgeben durch das übertragende Endgerät (hier M1) ausgeschlossen werden soll. Beim Umschalten, auch „switch“ genannt, wird der vom ersten Endgerät M1 erhaltene elektronische Münzdatensatz C_k gegen einen neuen elektronischen Münzdatensatz C_l mit gleichem monetärem Betrag ausgetauscht. Der neue elektronische Münzdatensatz C_l wird vom zweiten Endgerät M2 generiert. Dieses Umschalten ist notwendig, um die vom ersten Endgerät M1 erhaltenen elektronischen Münzdatensatz C_k zu invalidieren (ungültig machen), wodurch ein erneutes Ausgeben des gleichen elektronischen Münzdatensatzes C_k vermieden wird. Denn, solange der elektronische Münzdatensatz C_k nicht umgeschaltet ist, kann – da das erste Endgerät M1 in Kenntnis des elektronischen Münzdatensatzes C_k ist – das erste Endgerät M1 diesen elektronischen Münzdatensatz C_k an ein drittes Endgerät M3 weitergeben. Das Umschalten erfolgt beispielsweise durch Hinzufügen eines neuen Verschleierungsbetrags r_{add} zum Verschleierungsbetrag r_k des erhaltenen elektronischen Münzdatensatz C_k , wodurch ein Verschleierungsbetrag r_l erhalten wird, den nur das zweite Endgerät M2 kennt. Dies kann auch in

der Überwachungsinstanz 2 erfolgen. Um zu beweisen, dass ein neuer Verschleierungsbetrag r_{add} zum Verschleierungsbetrag r_k des maskierten erhaltenen elektronischen Münzdatensatzes Z_k hinzugefügt wurde, der monetäre Betrag aber gleichgeblieben ist, und also Gleichung (11):

$$v_k = v_l \quad (11)$$

5 gilt, so muss das zweite Endgerät M2 nachweisen können, dass sich $Z_l - Z_k$ als skalares Vielfaches von G also als $r_{add} * G$ darstellen lässt. Das heißt, dass nur ein Verschleierungsbetrag r_{add} erzeugt wurde und der monetäre Betrag von Z_l gleich dem monetären Betrag von Z_k ist, also $Z_l = Z_k + r_{add} * G$. Dies erfolgt durch das Erzeugen einer Signatur mit dem öffentlichen Schlüssel $Z_l - Z_k = r_{add} * G$. Diese
10 Signatur wird in der Überwachungsschicht 4 verwendet, um die Gültigkeit des umzuschaltenden elektronischen Münzdatensatzes zu bestätigen.

Die Modifikationen „Aufteilen“ und „Verbinden“ an einem elektronischen Münzdatensatz können auch von einem Endgerät M1 an ein anderes Endgerät M2, M3 delegiert werden, beispielsweise
15 wenn eine Kommunikationsverbindung zur Überwachungsinstanz 2 nicht vorhanden ist.

In Fig. 3 ist ein Ausführungsbeispiel eines Bezahlsystems gemäß der Erfindung zum „Aufteilen“, „Verbinden“ und „Umschalten“ von elektronischen Münzdatensätzen C gezeigt. In Fig. 3 hat das erste Endgerät M1 den Münzdatensatz C_i erhalten und möchte nun eine Bezahltransaktion nicht
20 mit dem gesamten monetären Betrag v_i , sondern nur mit einem Teilbetrag v_k durchführen. Dazu wird der Münzdatensatz C_i aufgeteilt. Dazu wird zunächst der monetäre Betrag geteilt:

$$v_i = v_j + v_k \quad (12)$$

Dabei muss jeder der erhaltenen Beträge v_j , v_k , größer 0 sein, denn negative monetäre Beträge sind
25 nicht zulässig.

Zudem werden neue Verschleierungsbeträge abgeleitet:

$$r_i = r_j + r_k \quad (13)$$

30 Bei einem Aufteilen werden maskierte Münzdatensätze Z_j und Z_k gemäß Gleichung (3) aus den Münzdatensätzen C_j und C_k erhalten und in der Überwachungsinstanz 2 registriert. Für das Aufteilen werden die Vorgängerspalte 22a mit dem Münzdatensatz Z_i , die Nachfolgerspalte 23a mit Z_j und die Nachfolgerspalte 23b mit Z_k beschrieben. Zusätzliche Informationen für den Bereichsnachweis (zero-knowledge-proof) sind zu generieren. Die Markierungen in den Spalten
35 25 bis 27 benötigen Statusänderung und die Überwachungsinstanz 2 führt die entsprechenden Prüfungen durch. Die Markierung gemäß Spalte 28 wird ignoriert.

Dann wird ein Münzteildatensatz, hier C_k , vom ersten Endgerät M1 an das zweite Endgerät M2 übertragen. Um ein doppeltes Ausgeben zu verhindern, ist eine Umschalt-Operation sinnvoll, um den vom ersten Endgerät M1 erhaltenen elektronischen Münzdatensatz C_k gegen einen neuen elektronischen Münzdatensatz C_l mit gleichem monetären Betrag auszutauschen. Der neue elektronische Münzdatensatz C_l wird vom zweiten Endgerät M2 generiert. Dabei wird der monetäre Betrag des Münzdatensatzes C_l übernommen und nicht verändert, siehe Gleichung (11).

Dann wird gemäß Gleichung (14) ein neuer Verschleierungsbetrag r_{add} zum Verschleierungsbetrag r_k des erhaltenen elektronischen Münzdatensatz C_k hinzugefügt,

$$r_l = r_k + r_{add} \quad (14)$$

wodurch ein Verschleierungsbetrag r_l erhalten wird, die nur das zweite Endgerät M2 kennt. Um zu beweisen, dass nur ein neuer Verschleierungsbetrag r_{add} zum Verschleierungsbetrag r_k des erhaltenen elektronischen Münzdatensatz Z_k hinzugefügt wurde, der monetäre Betrag aber gleichgeblieben ist ($v_k = v_l$), muss das zweite Endgerät M2 nachweisen können, dass sich $Z_l - Z_k$ als Vielfaches von G darstellen lässt. Dies erfolgt mittels öffentlicher Signatur R_{add} gemäß Gleichung (15):

$$\begin{aligned} R_{add} &= r_{add} \cdot G \\ &= Z_l - Z_k = (v_l - v_k) \cdot H + (r_k + r_{add} - r_k) \cdot G \end{aligned} \quad (15)$$

wobei G der Generatorpunkt der ECC ist. Dann wird der umzuschaltende Münzdatensatz C_l maskiert mittels der Gleichung (3) oder der Gleichung (3a), um den maskierten Münzdatensatz Z_l zu erhalten. In der Überwachungsinstanz 2 kann dann die private Signatur r_{add} genutzt werden um beispielsweise den maskierten umzuschaltenden elektronischen Münzdatensatz Z_l zu signieren, was als Beweis gilt, dass das zweite Endgerät M2 nur ein Verschleierungsbetrag r_{add} zum maskierten elektronischen Münzdatensatz hinzugefügt hat und keinen zusätzlichen monetären Wert, d.h. $v_l = v_k$.

Der Beweis lautet für Maskierungen mittels Gleichung (3) wie folgt:

$$\begin{aligned} Z_k &= v_k \cdot H + r_k \cdot G \\ Z_l &= v_l \cdot H + r_l \cdot G = v_k \cdot H + (r_k + r_{add}) \cdot G \\ Z_l - Z_k &= (r_k + r_{add} - r_k) \cdot G \\ &= r_{add} \cdot G \end{aligned} \quad (16)$$

Für eine Maskierung mittels der Gleichung (3a) wird eine Signatur über dem monetären Betrag v_k , dem Verschleierungsbetrag r_k und dem maskierten Münzdatensatzelement (bspw. dem maskierten

Verschleierungsbetrag R oder dem maskierten ersten Betragsteil) erzeugt. So kann die Signatur durch Neuberechnen der Maskierung in der Überwachungsinstanz 4 validiert werden, um die Echtheit und das Vorhandensein/Besitz des Münzdatensatzes C beweisen zu können.

5 Fig. 4 zeigt ein Ausführungsbeispiel eines Bezahlsystems gemäß der Erfindung zum Verbinden von elektronischen Münzdatensätzen. Dabei werden im zweiten Endgerät $M2$ die beiden Münzdatensätze C_i und C_j erhalten. In Anlehnung an das Aufteilen gemäß Fig. 3 wird nun ein neuer Münzdatensatz Z_m erhalten, indem sowohl die monetären Beträge als auch der Verschleierungsbetrag der beiden Münzdatensätze C_i und C_j addiert werden. Dann wird der
10 erhaltene zu verbindende Münzdatensatz C_m mittels der Gleichung (3) oder der Gleichung (3a) maskiert und der maskierte Münzdatensatz Z_m wird in der Überwachungsinstanz registriert.

Für Maskierungen mittels der Gleichung (3a) wird eine erste Signatur über den monetären Betrag v_i , dem Verschleierungsbetrag r_i und dem maskierten Münzdatensatz erzeugt und es wird eine
15 zweite Signatur über den monetären Betrag v_j , dem Verschleierungsbetrag r_j und dem maskierten Münzdatensatz Z_j erzeugt. Beide Signaturen können durch jeweiliges Neuberechnen der Maskierung in der Überwachungsinstanz 4 validiert werden, um die Echtheit und das Vorhandensein/Besitz des Münzdatensatzes C beweisen zu können. Die erste Signatur kann auch mit der zweiten Signatur verknüpft werden, um eine gemeinsame Signatur zu bilden.

20 Fig. 5 bis 7 ist jeweils ein Ausführungsbeispiel eines Verfahrensablaufdiagramms eines erfindungsgemäßen Verfahrens 100. Nachfolgend werden die Figuren 5 bis 7 gemeinsam erläutert. In den optionalen Schritten 101 und 102 wird ein Münzdatensatz angefragt und seitens der Herausgeberinstanz 1 dem ersten Endgerät $M1$ nach Erstellen des elektronischen Münzdatensatzes bereitgestellt. Ein signierter maskierter elektronischer Münzdatensatz wird im Schritt 103 an die
25 Überwachungsinstanz 2 gesendet. Im Schritt 103 erfolgt ein Maskieren des erhaltenen elektronischen Münzdatensatzes C_i gemäß der Gleichung (3) und wie in Fig. 1 erläutert. Dann wird im Schritt 104 der maskierte elektronische Münzdatensatz Z_i in der Überwachungsinstanz 2 registriert. Optional kann $M1$ den erhaltenen elektronischen Münzdatensatz umschalten. Im Schritt
30 105 erfolgt das Übertragen des Münzdatensatzes C_i in der Direkttransaktionsschicht 3 an das zweite Endgerät $M2$. In den optionalen Schritten 106 und 107 erfolgt eine Validitätsprüfung mit vorheriger Maskierung, bei der im Gutfall die Überwachungsinstanz 2 die Gültigkeit des Münzdatensatzes Z_i bzw. C_i bestätigt wird.

35 Im Schritt 108 erfolgt das Umschalten eines erhaltenen Münzdatensatzes C_k (es könnte natürlich auch der erhaltene Münzdatensatz C_i umgeschaltet werden) auf einen neuen Münzdatensatz C_l , wodurch der Münzdatensatz C_k ungültig wird und ein Doppeltausgeben verhindert wird. Dazu wird der monetäre Betrag v_k des übertragenen Münzdatensatzes C_k als „neuer“ monetärer Betrag v_l verwendet. Zudem wird, wie bereits mit Gleichungen (14) bis (17) erläutert, der

Verschleierungsbetrag r_1 erstellt. Der zusätzliche Verschleierungsbetrag r_{add} wird verwendet, um zu beweisen, dass kein neues Geld (in Form eines höheren monetären Betrags) von dem zweiten Endgerät M2 generiert wurde. Dann wird unter anderem der maskierte umzuschaltende Münzdatensatz Z_1 an die Überwachungsinstanz 2 gesendet und das Umschalten von C_k auf C_i beauftragt.

Im Schritt 108' erfolgt die entsprechende Prüfung in der Überwachungsinstanz 2. Dabei wird Z_k in die Spalte 22a gemäß Tabelle in Fig. 2 eingetragen und in Spalte 23b der umzuschreibende Münzdatensatz Z_1 . Es erfolgt sodann eine Prüfung in der Überwachungsinstanz 2, ob Z_k (noch) gültig ist, also ob die letzte Verarbeitung von Z_k in einer der Spalten 23a/b eingetragen ist (als Beweis dafür, dass Z_k nicht weiter aufgeteilt oder deaktiviert oder verbunden wurde) und ob eine Prüfung für die letzte Verarbeitung fehlgeschlagen ist. Zudem wird Z_1 in die Spalte 23b eingetragen und die Markierungen in den Spalten 25, 26, 27 werden zunächst auf „0“ gesetzt. Nun erfolgt eine Prüfung, ob Z_1 gültig ist, wobei dabei die Prüfung gemäß Gleichungen (16) und (17) verwendet werden können. Im Gutfall wird die Markierung in Spalte 25 auf „1“ gesetzt, ansonsten auf „0“. Nun erfolgt eine Prüfung, die Berechnung gemäß Gleichung (10) ergibt, dass Z_k und Z_1 gültig sind und entsprechend wird die Markierung in Spalte 26 gesetzt. Weiterhin wird geprüft, ob die Bereiche schlüssig sind, sodann wird die Markierung in Spalte 27 gesetzt. Wenn alle drei Prüfungen erfolgreich waren, und dies entsprechend unveränderlich in der Überwachungsinstanz 2 festgehalten wurde, gilt der Münzdatensatz als umgeschaltet. D.h. der Münzdatensatz C_k ist nicht mehr gültig und ab sofort ist der Münzdatensatz C_i gültig. Ein Doppeltausgeben ist nicht mehr möglich, wenn ein drittes Endgerät M3 die Validität des (doppelt ausgegebenen) Münzdatensatz an der Überwachungsinstanz 2 erfragt.

Im Schritt 109 erfolgt ein Verbinden von zwei Münzdatensätzen C_k und C_i auf einen neuen Münzdatensatz C_m , wodurch die Münzdatensätze C_k , C_i ungültig werden und ein Doppeltausgeben verhindert wird. Dazu wird der monetäre Betrag v_m aus den beiden monetären Beträgen v_k und v_i gebildet. Dazu wird der Verschleierungsbetrag r_m aus den beiden Verschleierungsbeträgen r_k und r_i gebildet. Zudem wird mittels Gleichung (3) der maskierte zu verbindende Münzdatensatz erhalten und dieser (mit anderen Informationen zusammen) an die Überwachungsinstanz 2 gesendet und das Verbinden als Verarbeitung erbeten.

Im Schritt 109' erfolgt die entsprechende Prüfung in der Überwachungsinstanz 2. Dabei wird Z_m in die Spalte 23b gemäß Tabelle in Fig. 2 eingetragen, was auch gleich einer Umschreibung. Es erfolgt sodann eine Prüfung in der Überwachungsinstanz 2, ob Z_k und Z_i (noch) gültig sind, also ob die letzte Verarbeitung von Z_k oder Z_i in einer der Spalten 23a/b eingetragen ist (als Beweis dafür, dass Z_k und Z_i nicht weiter aufgeteilt oder deaktiviert oder verbunden wurden) und ob eine Prüfung für die letzte Verarbeitung fehlgeschlagen ist. Zudem werden die Markierungen in den Spalten 25, 26, 27 zunächst auf „0“ gesetzt. Nun erfolgt eine Prüfung, ob Z_m gültig ist, wobei dabei

die Prüfung gemäß Gleichungen (16) und (17) verwendet werden können. Im Gutfall wird die Markierung in Spalte 25 auf „1“ gesetzt, ansonsten auf „0“. Nun erfolgt eine Prüfung, die Berechnung gemäß Gleichung (10) ergibt, dass Z_i plus Z_k gleich Z_m ist und entsprechend wird die Markierung in Spalte 26 gesetzt. Weiterhin wird geprüft, ob die Bereiche schlüssig sind, sodann wird die Markierung in Spalte 27 gesetzt.

Im Schritt 110' erfolgt die entsprechende Prüfung in der Überwachungsinstanz 2. Dabei werden Z_j und Z_k in die Spalten 23a/b gemäß Tabelle in Fig. 2 eingetragen. Es erfolgt sodann eine Prüfung in der Überwachungsinstanz 2, ob Z_i (noch) gültig ist, also ob die letzte Verarbeitung von Z_i in einer der Spalten 23a/b eingetragen ist (als Beweis dafür, dass Z_i nicht weiter aufgeteilt oder deaktiviert oder verbunden wurde) und ob eine Prüfung für die letzte Verarbeitung fehlgeschlagen ist. Zudem werden die Markierungen in den Spalten 25, 26, 27 zunächst auf „0“ gesetzt. Nun erfolgt eine Prüfung, ob Z_j und Z_k gültig sind, wobei dabei die Prüfung gemäß Gleichungen (16) und (17) verwendet werden können. Im Gutfall wird die Markierung in Spalte 25 auf „1“ gesetzt. Nun erfolgt eine Prüfung, die Berechnung gemäß Gleichung (10) ergibt, dass Z_i gleich Z_k plus Z_j ist und entsprechend wird die Markierung in Spalte 26 gesetzt. Weiterhin wird geprüft, ob die Bereiche schlüssig sind, sodann wird die Markierung in Spalte 27 gesetzt.

In Fig. 8 ist ein Ausführungsbeispiel eines erfindungsgemäßen Geräts M1 gezeigt. Das Gerät M1 kann elektronische Münzdatensätze C_i in einem Datenspeicher 10, 10' ablegen. Dabei können die elektronischen Münzdatensätze C_i auf dem Datenspeicher 10 des Geräts M1 liegen oder in einem externen Datenspeicher 10' verfügbar sein. Bei Verwenden eines externen Datenspeichers 10' könnten die elektronischen Münzdatensätze C_i in einem Online-Speicher abgelegt sein, beispielsweise einem Datenspeicher 10' eines Anbieters für digitale Geldbörsen. Zusätzlich könnten auch private Datenspeicher, bspw. ein Network-Attached-Storage, NAS in einem privaten Netzwerk verwendet werden.

In einem Fall ist der elektronische Münzdatensatz C_i als ein Ausdruck auf Papier dargestellt. Dabei kann der elektronische Münzdatensatz durch einen QR-Code, ein Bild eines QR-Codes dargestellt werden, oder aber auch eine Datei oder eine Zeichenfolge (ASCII) sein.

Das Gerät M1 hat mindestens eine Schnittstelle 12 als Kommunikationskanal zum Ausgeben des Münzdatensatzes C_i zur Verfügung. Diese Schnittstelle 12 ist beispielsweise eine optische Schnittstelle, beispielsweise zum Darstellen des Münzdatensatzes C_i auf einer Anzeigeeinheit (Display), oder einen Drucker zum Ausdrucken des elektronischen Münzdatensatzes C_i als Papier-Ausdruck. Diese Schnittstelle 12 kann auch eine digitale Kommunikationsschnittstelle, beispielsweise für Nahfeldkommunikation, wie NFC, Bluetooth, oder eine Internetfähige Schnittstelle, wie TCP, IP, UDP, HTTP oder ein Zugriff auf eine Chipkarte als Sicherheitselement sein. Diese Schnittstelle 12 ist beispielsweise eine Datenschnittstelle, sodass der Münzdatensatz

C_i über eine Applikation, beispielsweise einem Instant-Messenger-Dienst oder als Datei oder als Zeichenfolge zwischen Geräten übertragen wird.

5 Zudem ist die Schnittstelle 12 oder eine weitere Schnittstelle (nicht dargestellt) des Geräts M1 dazu eingerichtet, mit der Überwachungsinstanz 2 gemäß der Beschreibung in den Figuren 1 bis 6 zu interagieren. Das Gerät M1 ist dazu bevorzugt onlinefähig.

10 Darüber hinaus kann das Gerät M1 auch eine Schnittstelle zum Empfang von elektronischen Münzdatensätzen aufweisen. Diese Schnittstelle ist eingerichtet visuell präsentierte Münzdatensätze, beispielsweise mittels Erfassungsmodul wie Kamera oder Scanner, oder digital präsentierte Münzdatensätze, empfangen via NFC, Bluetooth, TCP, IP, UDP, HTTP oder mittels einer Applikation präsentierte Münzdatensätze zu empfangen.

15 Das Gerät M1 umfasst auch eine Recheneinheit 13, die das oben beschriebene Verfahren zum Maskieren von Münzdatensätzen und die Verarbeitungen an Münzdatensätzen durchführen kann.

20 Das Gerät M1 ist onlinefähig und kann bevorzugt mittels eines Standorterkennungs-Moduls 15 erkennen, wenn es mit einem WLAN verbunden ist. Optional kann ein spezifisches WLAN Netz als bevorzugt markiert sein (=Standortzone), sodass das Gerät M1 besondere Funktionen nur ausführt, wenn es in diesem WLAN Netz angemeldet ist. Alternativ erkennt das Standorterkennungs-Modul 15, wenn das Gerät M1 in vordefinierten GPS-Koordinaten inklusive eines definierten Radius ist und führt die besonderen Funktionen entsprechend der so definierten Standortzone durch. Diese Standortzone kann entweder manuell in das Gerät M1 oder via andere Einheiten/Module in das Gerät M1 eingebracht werden. Die besonderen Funktionen, die das Gerät 25 M1 bei Erkennen der Standortzone durchführt, sind insbesondere das Übertragen von elektronischen Münzdatensätzen von/zum externen Datenspeicher 10 von/zu einem Tresormodul 14 und ggf. das Übertragen maskierter Münzdatensätze Z an die Überwachungsinstanz 2, beispielsweise im Rahmen von den o.g. Verarbeitungen an einem Münzdatensatz.

30 Im einfachsten Fall werden im Endgerät M1 alle Münzdatensätze C_i nach Erhalt automatisch zu einem Münzdatensatz verbunden (siehe Verbinden-Verarbeitung bzw. Verbinden-Schritt). Das heißt, sobald ein neuer elektronischer Münzdatensatz empfangen wird, wird ein Verbinden bzw. Umschalten-Befehl an die Überwachungsinstanz 2 gesendet. Das Gerät M1 kann elektronische Münzdatensätze auch in algorithmisch festgelegten Denominationen vorbereiten und im 35 Datenspeicher 10, 10' vorhalten, damit auch ohne Datenverbindung zur Überwachungsinstanz 2 ein Bezahlvorgang möglich ist.

Fig. 9 und 10 zeigen jeweils ein Ausführungsbeispiel eines Verfahrensablaufdiagramms eines erfindungsgemäßen Verfahrens 200. Nachfolgend werden die Figuren 9 und 10 gemeinsam

erläutert. Die zuvor getroffenen Aussagen aus dem Verfahren 100 und den einzelnen Verfahrensschritten 101 bis 110 gelten auch für dieses Verfahren 200, es sei denn, es werden hier andere Aussagen getroffen.

- 5 In den optionalen Schritten 101 und 102 wird ein Münzdatensatz angefragt und seitens der Herausgeberinstanz 1 dem ersten Endgerät M1 nach Erstellen des elektronischen Münzdatensatzes bereitgestellt, siehe auch Fig.5 bis 7. Das erste Endgerät M1 überträgt im Schritt 105 die Münze C an das zweite Endgerät. Die hier dargestellten Verfahrensschritte 201 bis 208 werden zwar in Bezug auf das zweite Endgerät M2 erläutert, könnten aber auch im ersten Endgerät M1
10 durchgeführt werden. Das erste Endgerät M1 überträgt im Schritt 105 die Münze C_k an das zweite Endgerät.

Im Schritt 201 erfolgt das Auswählen eines Maskierungsmodus. Um ein doppeltes Ausgeben zu verhindern, ist eine Umschalt-Operation (Switch) vorgesehen, um den vom ersten Endgerät M1 erhaltenen elektronischen Münzdatensatz C_k gegen einen neuen elektronischen Münzdatensatz C_l
15 mit gleichem monetärem Betrag auszutauschen. Der neue elektronische Münzdatensatz C_l wird vom zweiten Endgerät M2 generiert. Dabei wird der monetäre Betrag v_k des Münzdatensatzes C_k übernommen und wird nicht verändert zum neuen monetären Betrag v_l , siehe Gleichung (11). Dann wird gemäß Gleichung (14) ein neuer Verschleierungsbetrag r_{add} zum Verschleierungsbetrag
20 r_k des erhaltenen elektronischen Münzdatensatz C_k hinzugefügt, wodurch ein Verschleierungsbetrag r_l erhalten wird, die nur das zweite Endgerät M2 kennt.

Die Auswahl des Maskierungsmodus erfolgt beispielsweise durch einen Benutzer des ersten Endgeräts M1 über eine entsprechende Menüsteuerung am Endgerät M1. Die Auswahl erfolgt
25 beispielsweise aufgrund einer Systemvorgabe x im Bezahlssystem. Beispielsweise kann so, eine Leistungsfähigkeit des Bezahlsystems optimal auszunutzen, sodass ein Aufwand der Nachweisprüfung (Schritt 207) auf Basis eines aktuellen Registrier-Anfragevolumen in der Überwachungsinstanz 2 durch entsprechende Auswahl des Maskierungsmodus steuern kann. Die Auswahl kann auch auf Basis einer Endgeräte-Eigenschaft gewählt werden, beispielsweise bei
30 fehlender Unterstützung eines der Maskierungsmodi kann eine entsprechende Vorauswahl getroffen werden.

Um nun den aufwendigen Nachweis der Gleichung (15) und (16) nicht durchführen zu müssen, wird nun gemäß Fig. 9 im optionalen Schritt 201 der vierte Maskierungsmodus gewählt. Es kann
35 im Schritt 202 der elektronische Münzdatensatz C_l entsprechend der Gleichung (3) maskiert werden, um den vollständig maskierten elektronischen Münzdatensatz Z_l gemäß zweitem Maskierungsmodus zu erhalten.

Im Schritt 203 wird optional eine erste Signatur mit dem Verschleierungsbetrag r_k als Signaturschlüssel gemäß Gleichung (17) erstellt:

$$[Z_k] \text{ sig } (r_k) \quad (17)$$

- 5 Zudem wird im Schritt 203 optional eine zweite Signatur mit der Differenz der Verschleierungsbeträge r_k und r_l als Signaturschlüssel gemäß Gleichung (18) erstellt:

$$[Z_k] \text{ sig } (r_l - r_k) \quad (18)$$

- 10 Im Schritt 203 kann der monetäre Betrag v_k des empfangenen elektronischen Münzdatensatz C_k zur ersten Signatur hinzugefügt werden, hier beispielhaft logisch verknüpft gemäß Gleichung (19) oder als Konkatenation gemäß Gleichung (19a):

$$v_k || \text{sig } (r_k) \quad (19)$$

$$v_k \circ \text{sig } (r_k) \quad (19a)$$

- 15 Das Umschalten (Modifizieren) erfolgt bevorzugt vor dem Senden-Schritt 204. Der im Schritt 204 an die Überwachungsinstanz 2 gesendete entsprechende unvollständig maskierte elektronische Münzdatensatz wird zusammen mit zumindest auch dem unmaskierten Münzdatensatzelement aus Gleichung (19) bzw. Gleichung (19a) und ggf. der zweiten Signatur aus Gleichung (18) versendet gemäß Gleichung (20) durch bloßes Hintereinander-Anordnen („;“ oder als Konkatenation „||“ gemäß Gleichung 20a :

$$v_k || \text{sig } (r_k); \text{ sig } (r_l - r_k); Z_l \quad (20)$$

$$v_k || \text{sig } (r_k) \circ \text{sig } (r_l - r_k) \circ Z_l \quad (20a)$$

- 20 Wird keine Signatur im Schritt 203 erstellt, wird das unmaskierte Münzdatensatzelement – hier der monetäre Betrag v_k oder der identische monetäre Betrag v_l zum vollständig maskierten elektronischen Münzdatensatz Z_l gemäß Gleichung (20b) hinzugefügt:

$$25 \quad v_k \circ Z_l \text{ bzw. } v_l \circ Z_l \quad (20b)$$

- 30 In der Überwachungsinstanz kann durch die Auswahl des ersten Maskierungsmodus eine vereinfachte Bereichsprüfung erfolgen. Diese umfasst beispielsweise vier Prüfungen (wenn die Signaturen im Schritt 203 erzeugt werden). Die erste Prüfung ist das Prüfen der Gültigkeit (Validität) des umzuschaltenden unvollständig maskierten Münzdatensatzes. Dies erfolgt entsprechend der vorangegangenen beschriebenen Art.

Die optionale zweite Prüfung gemäß Schritt 206 dient der Verifizierung der (optionalen) ersten Signatur. Dazu wird aus dem unmaskierten monetären Betrag v_k der öffentliche Verifikationsschlüssel der ersten Signatur erstellt, mit:

$$Z_k' = Z_k - v_k * H \quad (21)$$

Mit dem in Gleichung (21) erzeugten öffentlichen Verifikationsschlüssel wird die erste Signatur geprüft:

$$Z_k' = \text{sig}(r_k) \quad (22)$$

- 10 Ist die zweite Prüfung erfolgreich, so ist nachgewiesen, dass der monetäre Betrag v_k zum maskierten Münzdatensatz Z_k gehört und das zweite Endgerät M2 den Verschleierungsbetrag r_k kennt.

- 15 Die optionale dritte Prüfung gemäß Schritt 207 dient der Verifizierung der (optionalen) zweiten Signatur. Dazu wird die Differenz aus dem maskierten umzuschaltenden elektronischen Münzdatensatz Z_l und dem maskierten erhaltenen Münzdatensatz Z_k gebildet:

$$Z_l - Z_k = \text{sig}(r_l - r_k) \quad (23)$$

- 20 Mit dem in Gleichung (23) erzeugten öffentlichen Verifikationsschlüssel wird die zweite Signatur geprüft. Ist die dritte Prüfung erfolgreich, so ist nachgewiesen, dass die Differenz der monetären Beträge v_k v_l null ergibt und damit nachgewiesen ist, dass kein neues/zusätzliches Geld generiert wurde.

- 25 Die vierte Prüfung ist dann eine sehr einfache Bereichsprüfung durch die Überwachungsinstanz 2:

$$v_{\min} \leq v_k \leq v_{\max} \quad (24)$$

- Das Prüfen des Aufteilens (als Modifizieren) eines Münzdatensatzes C_i erfolgt auf vergleichbare Weise, wie das Umschalten. Das erste Endgerät M1 überträgt beispielsweise im Schritt 105 die Münze C_i an das zweite Endgerät M2.

- 30 Im optionalen Schritt 201 erfolgt das Auswählen des Maskierungsmodus. Um die aufwendigen Nachweise der Gleichung (15) und (16) nicht durchführen zu müssen, wird beispielsweise gemäß Fig. 9 im Schritt 201 der vierte Maskierungsmodus gewählt. Anschließend wird im Schritt 202 der elektronische Münzdatensatz C_i entsprechend der Gleichung (6) und (7) aufgeteilt, um einen ersten Münzteildatensatz C_j und einen zweiten Münzteildatensatz C_k zu erhalten. Im Schritt 203 können
- 35

dann optional drei separate erste Signatur über die Verschleierungsbeträge r_i , r_j und r_k gemäß Gleichung (17) erstellt werden. Zudem kann jeder der monetären Beträge v_i v_j v_k zur entsprechenden ersten Signatur hinzugefügt werden, beispielhaft logisch verknüpft gemäß Gleichung (19) oder als Konkatenation gemäß Gleichung (19a), sodass folgende drei erste

5 Signaturen erhalten werden:

$$v_i || \text{sig}(r_i) \quad (19b)$$

$$v_j || \text{sig}(r_j) \quad (19c)$$

$$v_k || \text{sig}(r_k) \quad (19d)$$

Das Aufteilen (Modifizieren) erfolgt bevorzugt vor dem Senden-Schritt 204. Die im Schritt 204 an die Überwachungsinstanz 2 gesendete entsprechende unvollständigen maskierten elektronische Münzteildatensätze Z_k Z_j werden zusammen mit den unmaskierten Münzdatensatzelementen aus Gleichungen (19b), (19c), (19d) bzw. entsprechender Konkatenation gemäß Gleichung (19a) versendet:

10

$$v_k || \text{sig}(r_k); v_i || \text{sig}(r_i); v_j || \text{sig}(r_j); Z_j; Z_k \quad (25)$$

15 Wird keine Signatur im Schritt 203 erstellt, wird das jeweilige unmaskierte Münzdatensatzelement – hier die monetären Beträge v_i v_j v_k zum entsprechenden vollständig maskierten elektronischen Münzdatensatz Z_i Z_j Z_k gemäß Gleichung (25a) hinzugefügt:

$$v_i \circ Z_i \ v_j \circ Z_j \ v_k \circ Z_k \quad (25a)$$

20 In der Überwachungsinstanz 2 kann durch die Auswahl des vierten Maskierungsmodus eine vereinfachte Bereichsprüfung erfolgen. Diese umfasst hier ebenfalls beispielsweise vier Prüfungen. Die erste Prüfung ist das Prüfen der Gültigkeit (Validität) des umzuschaltenden unvollständig maskierten Münzdatensatzes. Dies erfolgt entsprechend der vorangegangenen beschriebenen Art.

25 Die optionale zweite Prüfung gemäß Schritt 206 dient der Verifizierung der (optionalen) ersten Signatur über dem Verschleierungsbetrag r_i des ungeteilten Münzdatensatz C_i . Die zweite Prüfung erfolgt gemäß Gleichungen (21) und (22). Ist die zweite Prüfung erfolgreich, so ist nachgewiesen, dass der monetäre Betrag v_i zum maskierten Münzdatensatz Z_i gehört und das zweite Endgerät M2

30 den Verschleierungsbetrag r_i kennt.

Die dritte Prüfung gemäß Gleichung (26) dient dem Nachweis, dass kein zusätzliches Geld generiert wurde mit:

$$(Z_j + Z_k) - Z_i == 0 \quad (26)$$

Die optionale vierte Prüfung ist dann eine Berechnung der jeweiligen öffentlichen Verifikationsschlüssel zum Prüfen der restlichen ersten Signaturen mit:

$$Z_j' = Z_j - v_j * H \quad (27)$$

$$Z_k' = Z_k - v_k * H \quad (28)$$

Mit den in Gleichungen (27) und (28) erzeugten öffentlichen Verifikationsschlüssel wird die jeweilige erste Signatur geprüft:

$$Z_k' = \text{sig}(r_k) \quad (29)$$

$$Z_j' = \text{sig}(r_j) \quad (30)$$

Ist die optionale vierte Prüfung erfolgreich, so ist nachgewiesen, dass der monetäre Betrag v_k zum maskierten Münzdatensatz Z_k gehört, dass der monetäre Betrag v_j zum maskierten Münzdatensatz Z_j gehört und das zweite Endgerät M2 die Verschleierungsbeträge r_k und r_j kennt. Schließlich kann eine sehr einfache Bereichsprüfung analog zu Gleichung (24) erfolgen.

Das Prüfen des Verbindens (als Modifizieren) von zwei Münzdatensätzen C_i und C_j zu einem verbundenen Münzdatensatzes C_m erfolgt auf vergleichbare Weise. Im optionalen Schritt 201 erfolgt das Auswählen des Maskierungsmodus. Um die aufwendigen Nachweise der Gleichung (15) und (16) nicht durchführen zu müssen, kann gemäß Fig. 9 im Schritt 201 der zweite Maskierungsmodus gewählt werden. Anschließend wird im Schritt 202 der verbundene elektronische Münzdatensatz C_m entsprechend der Gleichung (6) und (7) gebildet. Im Schritt 203 werden dann wiederum die drei separaten ersten gemäß Gleichungen (19a) bis (19c) gebildet

Das Verbinden (Modifizieren) erfolgt bevorzugt vor dem Senden-Schritt 204. Der im Schritt 204 an die Überwachungsinstanz 2 gesendete entsprechende unvollständige maskierte verbundene elektronische Münzdatensatz Z_m wird zusammen mit den unmaskierten Datenelementen aus Gleichungen (19b), (19c), (19d) bzw. entsprechender Konkatenation gemäß Gleichung (19a) versendet:

$$v_k || \text{sig}(r_k); v_i || \text{sig}(r_i); v_j || \text{sig}(r_j); Z_m \quad (31)$$

Wird keine Signatur im Schritt 203 erstellt, wird das jeweilige unmaskierte Münzdatensatzelement – hier die monetären Beträge v_m v_j v_k zum entsprechenden vollständig maskierten elektronischen Münzdatensatz Z_m Z_j Z_k gemäß Gleichung (31a) hinzugefügt:

$$v_m \circ Z_m \quad v_j \circ Z_j \quad v_k \circ Z_k \quad (31a)$$

In der Überwachungsinstanz 2 kann durch die Auswahl des zweiten Maskierungsmodus eine vereinfachte Bereichsprüfung erfolgen. Diese umfasst hier ebenfalls beispielsweise vier
5 Prüfungen. Die erste Prüfung ist das Prüfen der Gültigkeit (Validität) des umzuschaltenden unvollständig maskierten Münzdatensatzes. Dies erfolgt entsprechend der vorangegangenen beschriebenen Art.

Die optionale zweite Prüfung dient der Verifizierung der (optionalen) ersten Signatur über dem
10 Verschleierungsbetrag r_i des ungeteilten Münzdatensatz C_i . Die zweite Prüfung erfolgt gemäß den Gleichungen (21) und (22). Ist die zweite Prüfung erfolgreich, so ist nachgewiesen, dass der monetäre Betrag v_i zum maskierten Münzdatensatz Z_i gehört und das zweite Endgerät M2 den Verschleierungsbetrag r_i kennt.

15 Die dritte Prüfung erfolgt analog zur Gleichung (26) und dient als Nachweis, dass kein zusätzliches Geld generiert wurde.

Die optionale vierte Prüfung ist dann eine Berechnung der jeweiligen öffentlichen Verifikationsschlüssel zum Prüfen der restlichen optionalen ersten Signaturen analog zu den
20 Gleichungen (27) bis (30). Schließlich kann eine sehr einfache Bereichsprüfung analog zu Gleichung (24) erfolgen.

In Fig. 11 ist ein weiteres Ausführungsbeispiel eines Verfahrensablaufdiagramms eines erfindungsgemäßen Verfahrens 300 dargestellt. Das in Fig. 11 vorgestellte Verfahren kann
25 vollständig auf eines der zuvor beschriebenen Verfahren angewendet werden. Es ist im Rahmen der vereinfachten Nachweisprüfung für alle Maskierungsmodi anwendbar.

Das zweite Endgerät M2 ist im Besitz des elektronischen Münzdatensatzes C_i , beispielsweise durch Übertragen im Schritt 105. Das zweite Endgerät kann nun den Münzdatensatz C_i
30 entsprechend einer der vorhergehend beschriebenen Modifizierschritte, Aufteilen, Verbinden, Umschalten verarbeiten. Um eine Bereichsprüfung für eine Überwachungsinstanz 1 zu vereinfachen, werden die folgenden Schritte durchgeführt:

Im Endgerät M2 wird nach dem Maskierschritt (der vorhergehend beschriebenen Art) der
35 maskierte elektronische Münzdatensatz geteilt in:

$$Z_i = Z_j + Z_k = (v_j * H) + (v_k * 2^v * H + r_k * G) \quad (32)$$

- wobei v_j kleiner als ein Vorgabewert x ist. Der Vorgabewert x ist beispielsweise systembedingt vorgegeben oder wird durch ein Aushandeln zwischen zwei Teilnehmern am Bezahlssystem erhalten. Der Vorgabewert x kann als Bezahlssystemparameter fest sein oder variabel, beispielsweise zwischen Endgeräten ausgehandelt worden sein.

Eine bitweise Darstellung von x , unter der Annahme, dass

$$x = 2^y \quad (33)$$

- erfolgt als ein Beispiel für eine stellenwertbasierte Aufteilung des maskierten Münzteilsatzes Z_k in $Z_{k,d}$ mit der Basis 2 mit:

$$Z_k = \sum_{d=y}^{n-1} Z_{k,d} = \sum_{d=y}^{n-1} (v_{k,d} * 2^y * H + r_{k,d} * G) = \sum_{d=y}^{n-1} (a_k 2^d * H + r_k * G) \quad (34)$$

wobei $a_j \in \{0,1\}$ ist. Der Verschleierungsbetrag r wird gewählt mit:

$$r = \sum_{d=y}^{n-1} r_d \quad (35)$$

- Beispiel 1: Beispielsweise ist der maskierte erhaltene elektronische Münzdatensatz $Z_i = 22 * H + 64 * G$ und der Vorgabewert x ist acht. Eine bitweise Darstellung des geldwerten Betrags v_i ist 1 0 1 1 0 mit $y = 3$, siehe Schritt 301 in Fig. 11.

- Die bitweise Darstellung des geldwerten Betrags v_j ist dann 1 1 0 (als $v_j = 6$) und $Z_j = 6 * H$, betrachtet werden die rechten y -ten Bits des geldwerten Betrags v_i .

- Die bitweise Darstellung des geldwerten Betrags v_k ist dann 10000 (als $v_k = 16$) und $Z_j = 6 * H$, wenn die y -ten Bits des geldwerten Betrags von v_i gleich null gesetzt werden. Der zweite maskierte Münzteildatensatz Z_k ist dann:

$$\begin{aligned} Z_k &= 16 * H + 64 * G \\ &= (0 * 2^3 * H + 20 * G) + (1 * 2^4 * H + 44 * G) \\ &= Z_{k,3} + Z_{k,4} \end{aligned} \quad (36)$$

Die Nachweisprüfung ist dann wie folgt:

Das zweite Endgerät M2 versendet den monetären Betrag v_k und die Liste von $Z_{k,d}$ aus Gleichung (34) für $y \leq d < n$ zur Überwachungsinstanz 2 im Schritt 302. Die Überwachungsinstanz 2 prüft im Schritt 303, ob:

$$Z_i = \sum_{d=y}^{n-1} Z_{k,d} + v_j * H \quad (37)$$

5

Bei fehlgeschlagener Prüfung wird das Kommando zurückgewiesen. Bei erfolgreicher Prüfung wird nachgewiesen durch die Überwachungsinstanz 2 dass es für jedes $Z_{k,d}$ ein entsprechendes a_d mit „0“ oder „1“ gibt, ohne dass die Werte offengelegt werden. Eine Bereichsprüfung ist erfolgreich, wenn für jedes a_d ein Wert von „0“ oder „1“ vorliegt. Dazu wird eine Ringsignatur verwendet. Mit einer Ringsignatur kann jeder für zwei oder mehr öffentliche Schlüssel nachweisen, dass die dazu korrespondierenden privaten Schlüssel bekannt sind, nämlich:

10

Szenario 1: Es soll gelten:

$$Z_{k,d} = r_d * G \quad (38)$$

$$Z_{k,d}^{\prime} := -H + r_d * G \quad (39)$$

15

Dafür wird im zweiten Endgerät M2 im Schritt 304 eine Zufallszahl w erstellt und daraus berechnet:

$$e_1 := h(w * G) \quad (40)$$

wobei h eine Hashwertfunktion und G der Generatorpunkt der ECC Kurve ist. Anschließend erstellt das Endgerät M2 eine zweite Zufallszahl p_1 und berechnet:

20

$$e_0 := h(p_1 * G - e_1 * Z_{k,d}^{\prime}) \quad (41)$$

$$p_0 := w + e_0 * r_d \quad (42)$$

und sendet die Ringsignatur $\{e_0, p_0, p_0\}$ im Schritt 305 an die Überwachungsinstanz 2. Die Überwachungsinstanz 2 berechnet:

$$e_1 = h(p_0 * G - e_0 * Z_{k,d}^{\prime}) \quad (43)$$

25 Nach Ersetzen von p_0 mit Gleichung (39) und $Z_{k,d}$ mit (38) ergibt sich Gleichung (44):

$$e_1 = h((w + e_0 * r_d) * G - e_0 * r_d * G) = h(w * G), \quad (44)$$

was dem ursprünglichen e_1 entspricht, so wie es im zweiten Endgerät M2 definiert war. Die Überwachungsinstanz 2 berechnet:

$$e_0' = h(p * G - e_1 * Z_{k,d}) \quad (45)$$

5 und prüft, ob $e_0' = e_0$ stimmt. Unter der Annahme, dass

$$Z_{k,d}' = x * H + r_d * G \text{ und } x \text{ ungleich } 0 \quad (46)$$

gilt:

$$e_1 = h(p_0 * G - e_0 * Z_{k,d}) = h(w * G - e_0 * x * H) \quad (47)$$

10 wodurch feststeht, dass das zweite Endgerät M2 p_1 mit $e_0 = h(s_1 * G - e_1 * Z_{k,d})$.

Szenario 2:

$$Z_{k,d} = H + r_d * G \quad (48)$$

$$Z_{k,d}' := r_d * G \quad (49)$$

Dafür wird im zweiten Endgerät M2 im Schritt 307 eine Zufallszahl w erstellt und berechnet:

$$e_2 := h(w * G) \quad (50)$$

15 wobei h eine Hashwertfunktion und G der Generatorpunkt der ECC Kurve ist. Anschließend erstellt das Endgerät M2 eine zweite Zufallszahl p_0 und berechnet:

$$e_1 := h(p_0 * G - e_2 * Z_{k,d}) \quad (51)$$

$$p_1 := w + e_1 * r_d \quad (52)$$

Das Endgerät M2 berechnet im Schritt 307 auch:

$$20 \quad e_0 = h(p_1 * G - e_1 * Z_{k,d}') \quad (53)$$

Es ergibt sich

$$e_0 = h((w + e_1 * r_d) * G - e_1 * r_d * G) = h(w * G) = e_2 \quad (54)$$

25 Das Endgerät M2 sendet die Ringsignatur $\{e_0, p_0, p_1\}$ zur Überwachungsinstanz 2 im Schritt 308. Die Überwachungsinstanz 2 berechnet im Schritt 309:

$$\begin{aligned} e_1 &= h(p_0 * G - e_1 * Z_{k,d}) \\ e_0' &= h(p_1 * G - e_1 * Z_{k,d}) \end{aligned} \quad (55)$$

und prüft, ob $e_0' = e_0$ stimmt. Unter der Annahme, dass

$$Z_{k,d}' = x * H + r_d * G \text{ mit } x \text{ ungleich } 0 \quad (56)$$

5 gilt:

$$\begin{aligned} e_0 &= h(p_1 * G - e_1 * Z_{k,d}') \\ &= h((w + e_1 * r_d) * G - e_1 * r_d * G - e_1 * x * H) \\ &= h(k * G - e_1 * x * H) = e_2 \end{aligned} \quad (57)$$

wodurch feststeht, dass das zweite Endgerät M2 p_0 mit

$$\begin{aligned} e_1 &= h(p_0 * G - e_2 * Z_{k,d}) \\ &= h((p_0 - e_2 * r_d) * G - e_2 * H) \end{aligned} \quad (58)$$

finden muss.

10

Beispiel 2 wird figürlich nicht dargestellt und zeigt exemplarisch ein Beispiel, in dem der Stellenwert eine beliebige Basis hat, also entgegen dem Beispiel 1 keine Basis 2 hat. Unter der Annahme der Gleichung (34) gilt dann:

15 Eine stellwertweise Darstellung von x , unter der Annahme, dass b eine beliebige Basis ist

$$x = b^y \quad (59)$$

erfolgt als ein Beispiel für eine stellenwertbasierte Aufteilung des maskierten Münzteilsatzes Z_k in $Z_{k,d}$ mit:

20

$$Z_k = \sum_{d=y}^{n-1} Z_{k,d} = \sum_{d=y}^{n-1} (v_{2,d} * b^y * H + r_{2,d} * G) = \sum_{d=y}^{n-1} (a_d b^d * H + r_d * G) \quad (60)$$

wobei $a_j \in \{0, \dots, b\}$ ist. Der Verschleierungsbetrag r wird gewählt mit:

$$r = \sum_{d=y}^{n-1} r_d \quad (61)$$

Beispiel 2: Beispielsweise ist der maskierte erhaltene elektronische Münzdatensatz wiederum $Z_i = 22 * H + 64 * G$ (in Analogie zu Schritt 301), aber hier ist der Vorgabewert $x = 9$. Eine ternäre Darstellung des geldwerten Betrags v_i ist 2 1 1 mit $y = 2$.

- 5 Die ternäre Darstellung des geldwerten Betrags v_j ist dann 0 1 1 (als $v_j = 4$) und $Z_j = 4 * H$, betrachtet werden die rechten y -ten Bits des geldwerten Betrags v_i .

Die ternäre Darstellung des geldwerten Betrags v_k ist dann 200 (als $v_k = 18$), wenn die y -ten Stellen des geldwerten Betrags von v_i gleich null gesetzt werden. Der zweite maskierte Münzteildatensatz

10 Z_k ist dann:

$$\begin{aligned} Z_k &= 18 * H + 64 * G \\ &= (2 * 3^2 * H + 64 * G) \\ &= Z_{k,2} \end{aligned} \tag{62}$$

- Die Nachweisprüfung ist dann wie folgt. Das zweite Endgerät M2 versendet (in Analogie zu Schritt 302) den monetären Betrag v_k und die Liste von $Z_{k,d}$ aus Gleichung (34) für $y \leq d < n$ zur Überwachungsinstanz 2. Die Überwachungsinstanz 2 prüft (in Analogie zu Schritt 303) entsprechend der Gleichung (37).

- Bei fehlgeschlagener Prüfung wird das Kommando zurückgewiesen. Bei erfolgreicher Prüfung wird nachgewiesen durch die Überwachungsinstanz 2, dass es für jedes $Z_{k,d}$ ein entsprechendes a_d mit „0 oder n “ im Bereich von „0 < n < b “ gibt, ohne dass die Werte offengelegt werden. Eine Bereichsprüfung ist erfolgreich, wenn für jedes a_d ein Wert von $0 < n < b$ vorliegt. Dazu wird eine Ringsignatur verwendet. Mit einer Ringsignatur kann jeder für zwei oder mehr öffentliche Schlüssel nachweisen, dass einer der dazu korrespondierenden privaten Schlüssel bekannt sind, nämlich. Ringsignaturen sind in MAXWELL et.al. „Borromean Ring Signatures“, vom 14. Juni 2015, abrufbar unter:

https://github.com/Blockstream/borromean_paper/raw/master/borromean_draft_0.01_8c3f9e7.pdf

- beschrieben und es wird für das Erstellen und Anwenden und Prüfen der Ringsignaturen auf die gesamte Offenbarung in MAXWELL et.al. „Borromean Ring Signatures“ Bezug genommen.

- In Figuren 12 und 13 ist ein weiteres Ausführungsbeispiel eines erfindungsgemäßen Verfahrens 400 gezeigt, das den ersten Maskierungsmodus betrifft. Figuren 12 und 13 werden zusammen beschrieben. Die zuvor getroffenen Aussagen aus dem Verfahren 100, 200 und 300 und den einzelnen Verfahrensschritten gelten auch für dieses Verfahren 400, es sei denn, es werden hier andere Aussagen getroffen.

Zunächst wird das Erstellen eines Münzdatensatzes für das Verfahren 400 beschrieben. In den Schritten 101 und 102 wird ein Münzdatensatz angefragt und seitens der Herausgeberinstanz 1 dem ersten Endgerät M1 nach Erstellen des elektronischen Münzdatensatzes bereitgestellt, siehe auch Fig.5 bis 7. Der elektronische Münzdatensatz C_i hat beispielsweise die Struktur gemäß Gleichung (1). Die Herausgeberinstanz 1 berechnet zu dem elektronischen Münzdatensatz C_i einen quasimaskierten Münzdatensatz Z_i gemäß Gleichung (3a), der die Struktur gemäß Gleichung (63) hat:

$$Z_i = \{v_i; R_i\} \quad (63)$$

, wobei der Wert R_i gemäß der Gleichung (64) definiert ist:

$$R_i = r_i \cdot G \quad (64)$$

G ist – wie G der Gleichung (3) – ein Generatorpunkt einer elliptischen Kurvenverschlüsselung, ECC, – also ein privater Schlüssel der ECC. Die Herausgeberinstanz 1 signiert gemäß Gleichung (65) den quasi-maskierten Münzdatensatz Z_i unter Verwendung eines privaten Signaturschlüssels PK_1 der Herausgeberinstanz 1:

$$[v_i; R_i]_{sig}(PK_1) \quad (65)$$

Der signierte quasimaskierte elektronische Münzdatensatz wird im Schritt 103 an die Überwachungsinstanz 2 gesendet.

Für das Umschalten eines Münzdatensatzes C_k wird wie folgt vorgegangen. Das erste Endgerät M1 überträgt im Schritt 105 die Münze C_k an das zweite Endgerät M2. Die hier dargestellten Verfahrensschritte 401 bis 407 werden zwar in Bezug auf das zweite Endgerät M2 erläutert, könnten aber auch im ersten Endgerät M1 durchgeführt werden.

Im Schritt 401, der dem Schritt 201 des Verfahrens 200 entspricht, erfolgt (optional) das Auswählen eines Maskierungsmodus. Um ein doppeltes Ausgeben zu verhindern, ist eine Umschalt-Operation (Switch) vorgesehen, um den vom ersten Endgerät M1 erhaltenen elektronischen Münzdatensatz C_k gegen einen neuen elektronischen Münzdatensatz C_l mit gleichem monetärem Betrag auszutauschen. Der neue elektronische Münzdatensatz C_l wird vom zweiten Endgerät M2 generiert. Dabei wird der monetäre Betrag v_k des Münzdatensatzes C_k übernommen und wird nicht verändert zum neuen monetären Betrag v_l , siehe auch Gleichung (11).

Dann wird gemäß Gleichung (14) ein neuer Verschleierungsbetrag r_{add} zum Verschleierungsbetrag

r_k des erhaltenen elektronischen Münzdatensatz C_k hinzugefügt, wodurch ein Verschleierungsbetrag r_l erhalten wird, den nur das zweite Endgerät M2 kennt.

Die Auswahl gemäß Schritt 401 erfolgt beispielsweise durch einen Benutzer des ersten Endgeräts M1 über eine entsprechende Menüsteuerung am Endgerät M1. Die Auswahl erfolgt beispielsweise aufgrund einer Systemvorgabe anhand des Vorgabewertes x im Bezahlssystem BZ. Beispielsweise kann so, eine Leistungsfähigkeit des Bezahlsystems BZ optimal ausgenutzt werden, sodass ein Aufwand der Nachweisprüfung (siehe auch Schritt 207) auf Basis eines aktuellen Registrier-Anfragevolumen in der Überwachungsinstanz 2 durch entsprechende Auswahl des Maskierungsmodus gesteuert werden kann. Die Auswahl kann auch auf Basis einer Endgeräte-Eigenschaft gewählt werden, beispielsweise bei fehlender Unterstützung eines der Maskierungsmodi kann eine entsprechende Vorauswahl getroffen werden.

Um den aufwendigen Nachweis der Gleichung (15) und (16) nicht durchführen zu müssen, wird nun gemäß Fig. 12 im Schritt 401 der dritte Maskierungsmodus zum Erhalten eines quasi-maskierten elektronischen Münzdatensatzes gewählt. Anschließend wird im Schritt 402 der elektronische Münzdatensatz C_k entsprechend der Gleichungen (63), (64) maskiert, um den quasi-maskierten elektronischen Münzdatensatz Z_k zu erhalten. Zudem wird der Verschleierungsbetrag gemäß Gleichung (64) verschlüsselt.

Dann wird im Schritt 403 eine erste Signatur gemäß Gleichung (66) erstellt:

$$[Z_k; R_l] \text{sig}(r_k) \quad (66)$$

Diese erste Signatur wird über den im Schritt 402 erstellten quasi-maskierten elektronischen Münzdatensatz Z_k und den im Schritt 402 erstellten verschlüsselten Verschleierungsbetrag R_l mit dem Verschleierungsbetrag r_l als Signaturschlüssel der ersten Signatur erzeugt.

Das Umschalten (als Modifizieren) erfolgt bevorzugt vor dem Sende-Schritt 204. Der im Schritt 404 an die Überwachungsinstanz 2 gesendete quasi-maskierte elektronische Münzdatensatz Z_l wird zusammen mit der in Gleichung (66) erzeugten Signatur versendet.

In der Überwachungsinstanz 2 kann eine vereinfachte Bereichsprüfung erfolgen. Diese umfasst zwei Prüfungen. Die erste Prüfung gemäß Schritt 405 ist das Prüfen der Gültigkeit (Validität) des umzuschaltenden quasi-maskierten Münzdatensatzes. Dies erfolgt entsprechend der vorangegangenen beschriebenen Art.

Die zweite Prüfung gemäß Schritt 406 dient der Verifizierung der ersten Signatur. Dazu wird der verschlüsselte Verschleierungsbetrag R_l des quasi-maskierten Münzdatensatzes Z_l als öffentlicher

Verifikationsschlüssel der ersten Signatur verwendet und geprüft, ob die im Schritt 404 mit übertragene erste Signatur gemäß Gleichung (66) gültig ist. Sind beide Prüfungen erfolgreich, gilt der Münzdatensatz C_i als gültig und eine Registrierung durch die Überwachungsinstanz 2 erfolgt im Schritt 407.

5 Das Prüfen des Aufteilens (als Modifizieren) eines Münzdatensatzes C_i erfolgt auf vergleichbare Weise, wie das Umschalten. Das erste Endgerät M1 überträgt beispielsweise im Schritt 105 die Münze C_i an das zweite Endgerät M2.

10 Im Schritt 401 erfolgt das Auswählen des Maskierungsmodus. Um die aufwendigen Nachweise der Gleichung (15) und (16) nicht durchführen zu müssen, wird nun im Schritt 401 der dritte Maskierungsmodus gewählt. Anschließend wird im Schritt 402 der elektronische Münzdatensatz C_i entsprechend der Gleichung (6) und (7) aufgeteilt, um einen ersten Münzteildatensatz C_j und einen zweiten Münzteildatensatz C_k zu erhalten. Zudem werden die Verschleierungsbeträge r_i , r_k ,
15 r_l mittels der Gleichung (64) zu R_i , R_k und R_l verschlüsselt.

Dann wird im Schritt 403 eine erste Signatur gemäß Gleichung (67) erstellt:

$$[Z_i; Z_k; Z_l]sig(r_i) \quad (67)$$

20 Das Aufteilen (Modifizieren) erfolgt bevorzugt vor dem Senden-Schritt 404. Die im Schritt 404 an die Überwachungsinstanz 2 gesendeten quasimaskierten elektronischen Münzteildatensätze Z_k Z_j werden zusammen mit der ersten Signatur aus Gleichung (67) bzw. entsprechender Konkatenation (vgl. Gleichung (19a)) versendet:

$$[Z_i; Z_k; Z_l]sig(r_i); Z_j; Z_k \quad (68)$$

25 In der Überwachungsinstanz 2 kann nun eine vereinfachte Bereichsprüfung erfolgen. Diese umfasst hier vier Prüfungen. Die erste Prüfung ist das Prüfen der Gültigkeit (Validität) des umzuschaltenden unvollständig maskierten Münzdatensatzes. Dies erfolgt entsprechend der vorangegangenen beschriebenen Art.

30 Die zweite Prüfung gemäß Schritt 406 dient der Verifizierung der ersten Signatur. Dazu wird der verschlüsselte Verschleierungsbetrag R_i des quasimaskierten Münzdatensatzes Z_i als öffentlicher Verifikationsschlüssel der ersten Signatur verwendet und geprüft, ob die im Schritt 404 mit übertragene erste Signatur gemäß Gleichung (67) gültig ist.

35 Die dritte Prüfung gemäß Gleichung (69) dient dem Nachweis, dass kein zusätzliches Geld generiert wurde mit:

$$v_i == v_k + v_l \quad (69)$$

Die vierte Prüfung ist dann eine Bereichsprüfung in der Überwachungsinstanz 2 mit:

$$v_{min} \leq v_k \leq v_{max} \quad (70)$$

$$v_{min} \leq v_l \leq v_{max} \quad (71)$$

5

Sind alle vier Prüfung erfolgreich, wird der quasimaskierte Münzdatensatz Z_i ungültig und die Münzteildatensätze Z_k und Z_l gültig und entsprechendes in der Überwachungsinstanz registriert.

Das Prüfen des Verbindens (als Modifizieren) von zwei Münzdatensätzen C_i und C_j zu einem verbundenen Münzdatensatzes C_m erfolgt auf vergleichbare Weise. Im Schritt 401 erfolgt das Auswählen des Maskierungsmodus. Um die aufwendigen Nachweise der Gleichung (15) und (16) nicht durchführen zu müssen, wird im Schritt 401 der dritte Maskierungsmodus gewählt. Entsprechend der Gleichungen (63), (64) werden die Verschleierungsbeträge r_i , r_j , r_m mittels der Gleichung (64) zu R_i , R_j und R_m verschlüsselt, um Z_i , Z_j und Z_m zu erhalten. Dann wird im Schritt 403 eine erste Signatur gemäß Gleichung (72) erstellt:

15

$$[Z_i; Z_j; Z_m]sig(r_i) \quad (72)$$

Dann wird im Schritt 403 die erste Signatur gemäß Gleichung (72) erneut signiert:

$$[[Z_i; Z_j; Z_m]sig(r_i)]sig(r_j) \quad (73)$$

20

Das Verbinden (Modifizieren) erfolgt bevorzugt vor dem Senden-Schritt 404. Der im Schritt 404 an die Überwachungsinstanz 2 gesendete quasimaskierte elektronischen Münzteildatensatz Z_m wird zusammen mit der Signatur aus Gleichung (74) bzw. entsprechender Konkatenation (vgl. Gleichung (19a)) versendet:

25

$$[[Z_i; Z_j; Z_m]sig(r_i)]sig(r_j); Z_m \quad (74)$$

30

In der Überwachungsinstanz 2 kann nun eine vereinfachte Bereichsprüfung erfolgen. Diese umfasst hier vier Prüfungen. Die erste Prüfung ist das Prüfen der Gültigkeit (Validität) des umzuschaltenden unvollständig maskierten Münzdatensatzes. Dies erfolgt entsprechend der vorangegangenen beschriebenen Art.

Die zweite Prüfung gemäß Schritt 406 dient der Verifizierung der Signatur aus Gleichung (73) und der ersten Signatur aus Gleichung (72). Dazu wird der verschlüsselte Verschleierungsbetrag

R_i des quasimaskierten Münzdatensatzes Z_i bzw. der verschlüsselte Verschleierungsbetrag R_j des quasimaskierten Münzdatensatzes Z_j jeweils als öffentlicher Verifikationsschlüssel verwendet und geprüft, ob die im Schritt 404 mit übertragene(n) Signatur(n) gemäß Gleichungen (72) und (73) gültig sind.

- 5 Die dritte Prüfung gemäß Gleichung (75) dient dem Nachweis, dass kein zusätzliches Geld generiert wurde mit:

$$v_m == v_i + v_j \quad (75)$$

- 10 Die vierte Prüfung ist dann eine Bereichsprüfung in der Überwachungsinstanz 2 mit:

$$v_{min} \leq v_m \leq v_{max} \quad (76)$$

Sind alle vier Prüfung erfolgreich, werden quasimaskierten Münzdatensätze Z_i und Z_j ungültig und der Münzdatensatz Z_m gültig und entsprechendes in der Überwachungsinstanz 2 registriert.

- 15 Das Löschen eines Münzdatensatzes im Verfahren 400 ist in Fig. 12 und 13 nicht dargestellt. Zum Löschen sendet das Endgerät ein entsprechendes Löschen-Kommando an die Überwachungsinstanz 2. In der Überwachungsinstanz 2 wird die gemäß Gleichung (65) erstellte Signatur der Herausgeberinstanz 1 geprüft und bei Übereinstimmung erfolgt ein Ungültigmachen in der Überwachungsinstanz 2.

- 20 Im Rahmen der Erfindung können alle beschriebenen und/oder gezeichneten und/oder beanspruchten Elemente beliebig miteinander kombiniert werden.

BEZUGSZEICHENLISTE

- 1 Herausgeberinstanz oder Bank
 2 Überwachungsinstanz
 5 21 Befehls-Eintrag
 22a, b Eintrag eines zu verarbeitenden elektronischen Münzdatensatzes (Vorgänger)
 23a, b Eintrag eines verarbeiteten elektronischen Münzdatensatzes (Nachfolger)
 24 Signatur-Eintrag
 25 Markierung der Gültigkeitsprüfung
 10 26 Markierung der Berechnungsprüfung
 27 Markierung der Bereichsnachweisprüfung
 28 Markierung der Signatur-Prüfung
 3 Direkttransaktionsschicht
 4 Überwachungsschicht
 15 5 Applikation gemeinsame Geldbörse
 10, 10' Datenspeicher
 11 Anzeige
 12 Schnittstelle
 13 Recheneinheit
 20 14 Tresormodul
 15 Standorterkennungs-Modul
 M1 erstes Endgerät
 M2 zweites Endgerät
 M3 drittes Endgerät
 25 C_i elektronischer Münzdatensatz
 C_j, C_k aufgeteilter elektronischer Münzteildatensatz,
 C_l umzuschaltender elektronischer Münzdatensatz
 C_m zu verbindender/verbundener elektronischer Münzdatensatz
 Z_i maskierter elektronischer Münzdatensatz
 30 Z_j, Z_k maskierter aufgeteilter elektronischer Münzteildatensatz
 Z_l maskierter umzuschaltender elektronischer Münzdatensatz
 Z_m maskierter zu verbindender elektronischer Münzdatensatz
 v_i Monetärer Betrag
 v_j, v_j Aufgeteilter monetärer Betrag
 35 v_l Monetärer Betrag eines umzuschaltenden/umgeschalteten elektr. Münzdatensatzes
 v_m Monetärer Betrag eines zu verbindenden/verbundenen elektr. Münzdatensatz
 r_i Verschleierungsbetrag, Zufallszahl
 r_j, r_j Verschleierungsbetrag eines aufgeteilten elektronischen Münzdatensatzes
 r_m Verschleierungsbetrag eines zu verbindenden/verbundenen elektronischen
 40 Münzdatensatzes
 C_i^{*} übertragener elektronischer Münzdatensatz
 C_j^{*}, C_k^{*} übertragener aufgeteilter elektronischer Münzteildatensatz,

- Z_i^* maskierter übertragener elektronischer Münzdatensatz
 Z_j^*, Z_k^* maskierter übertragener aufgeteilter elektronischer Münzdatensatz
 R maskierter Verschleierungsbetrag
 $f(C)$ (Homomorphe) Einwegfunktion
- 5 $[Z_i]Sig$ Signatur der Herausgeberinstanz
 Sig öffentlicher Verifikationsschlüssel der Signatur
 sig privater Signaturschlüssel der Signatur
 w Zufallszahl
 e, p Element der Ringsignatur
- 10 x Vorgabewert
101-108 Verfahrensschritte gemäß einem Ausführungsbeispiel
201-208 Verfahrensschritte gemäß einem Ausführungsbeispiel
301-309 Verfahrensschritte gemäß einem Ausführungsbeispiel
401-407 Verfahrensschritte gemäß einem Ausführungsbeispiel

PATENTANSPRÜCHE

1. Ein Verfahren zum direkten Übertragen von elektronischen Münzdatensätzen (C_i, C_j, C_k, C_m, C_l) zwischen Endgeräten (M1, M2, M3) zum Bezahlen in einem Bezahlssystem, wobei ein erstes
- 5 Endgerät (M1) zumindest einen elektronischen Münzdatensatz (C_i, C_j, C_k) aufweist, wobei der zumindest eine elektronische Münzdatensatz (C_i, C_j, C_k) einen monetären Betrag (v_i, v_j, v_k) und einen Verschleierungsbetrag (r_i, r_j, r_k) als Münzdatensatzelemente aufweist, mit den Schritten:
- Maskieren (202) eines ersten Münzdatensatzelements des elektronischen Münzdatensatzes (C_i, C_j, C_k), bevorzugt im ersten Endgerät (M1), durch Anwenden einer Einwegfunktion, die
- 10 beispielsweise homomorph ist, auf das erste Münzdatensatzelement des elektronischen Münzdatensatzes (C_i, C_j, C_k) zum Erhalten eines maskierten ersten elektronischen Münzdatensatzelements;
- Hinzufügen eines zweiten Münzdatensatzelements des elektronischen Münzdatensatzes (C_i, C_j, C_k) zu dem maskierten ersten elektronischen Münzdatensatzelement, bevorzugt im ersten
- 15 Endgerät (M1), zum Erhalten eines quasi-maskierten elektronischen Münzdatensatzes (Z_j, Z_j, Z_k); und
- Senden (207) des quasi-maskierten elektronischen Münzdatensatzes (Z_j, Z_j, Z_k) an eine Überwachungsinstanz (2) zum Registrieren des elektronischen Münzdatensatzes (C_i, C_j, C_k).
- 20 2. Das Verfahren nach Anspruch 1, wobei das erste Münzdatensatzelement der Verschleierungsbetrag (r_i, r_j, r_k) des elektronischen Münzdatensatzes (C_i, C_j, C_k) ist.
3. Das Verfahren nach einem der vorhergehenden Ansprüche, wobei das zweite Münzdatensatzelement:
- 25 - der monetäre Betrag (v_i, v_j, v_k) des elektronischen Münzdatensatzes (C_i, C_j, C_k) ist, wodurch ein betragsteiloffener maskierter elektronischer Münzdatensatz als der quasi-maskierte elektronische Münzdatensatz erhalten wird, oder
- ein höherwertiger Betragsanteil des stellenweise in den höherwertigen und einen niederwertigen Betragsanteil aufgeteilten monetären Betrages des elektronischen
- 30 Münzdatensatzes ist, wodurch ein nur hinsichtlich des höherwertigen Betragsanteils betragsteiloffener elektronischer Münzdatensatz als der quasi-maskierte elektronische Münzdatensatz erhalten wird.
4. Das Verfahren nach einem der vorhergehenden Ansprüche, wobei das Verfahren weiter
- 35 umfasst:
- Festlegen (201) eines Maskierungsmodus aus zumindest zwei Maskierungsmodi, wobei in einem ersten Maskierungsmodus der quasi-maskierte elektronische Münzdatensatz (Z_j, Z_j, Z_k) gesendet (207) wird und wobei in einem zweiten Maskierungsmodus der elektronische

Münzdatensatz (C_i, C_j, C_k), bevorzugt im ersten Endgerät (M1), durch Anwenden einer Einwegfunktion ($f(C)$), die beispielsweise homomorph ist, auf den elektronischen Münzdatensatz (C_i, C_j, C_k) zum Erhalten eines vollständig maskierten elektronischen Münzdatensatzes (Z_j, Z_j, Z_k) maskiert wird und der vollständig maskierte elektronische Münzdatensatz (Z_j, Z_j, Z_k) gesendet (207) wird.

5. Das Verfahren nach Anspruch 4, wobei:

ein dritter Maskierungsmodus umfasst: stellenwertweises Aufteilen des monetären Betrags (v_i, v_j, v_k) des elektronischen Münzdatensatzes (C_i, C_j, C_k), bevorzugt im ersten Endgerät, in einen ersten monetären Betragsteil und in einen zweiten monetären Betragsteil, wobei die Basis des Stellenwerts beliebig ist; Maskieren (202) des ersten monetären Betragsteils des monetären Betrags des elektronischen Münzdatensatzes (C_i, C_j, C_k), bevorzugt im ersten Endgerät (M1), durch Anwenden der Einwegfunktion ($f(C)$) auf den ersten monetären Betragsteil des monetären Betrags des elektronischen Münzdatensatzes (C_i, C_j, C_k) zum Erhalten eines maskierten ersten monetären Betragsteils und Hinzufügen des zweiten monetären Betragsteils zu dem maskierten ersten monetären Betragsteils zum Erhalten eines teilbetragsmaskierten elektronischen Münzdatensatzes.

6. Das Verfahren nach Anspruch 4 oder 5, wobei der Schritt des Registrierens (207) in Abhängigkeit des festgelegten Maskierungsmodus entweder das Registrieren des vollständig maskierten elektronischen Münzdatensatzes (Z_j, Z_j, Z_k) oder des quasi-maskierten elektronischen Münzdatensatzes oder des teilbetragsmaskierten elektronischen Münzdatensatzes in der Überwachungsinstanz (2) ist.

7. Das Verfahren nach einem der Ansprüche 4 bis 6, wobei der Schritt des Festlegens durch ein Auswählen des Maskierungsmodus im ersten Endgerät (M1) erfolgt, wobei bevorzugt ein Parameter zum Festlegen des Maskierungsmodus von der Überwachungsinstanz (2) oder einem Diensteanbieter vorgegeben ist und das Endgerät den Maskierungsmodus anhand dieses Parameters auswählt.

8. Das Verfahren nach einem der vorhergehenden Ansprüche 4 bis 7, wobei der Schritt des Festlegens durch ein Auswählen des Maskierungsmodus in der Überwachungsinstanz (2) oder durch einen Diensteanbieter erfolgt.

9. Das Verfahren nach einem der vorhergehenden Ansprüche, wobei der Maskierungsmodus für einen elektronischen Münzdatensatz gewechselt wird.

10. Das Verfahren nach einem der vorhergehenden Ansprüche mit den weiteren Verfahrensschritten:

- Erzeugen einer Signatur unter Verwendung des Verschleierungsbetrags (r_i , r_j , r_k) des elektronischen Münzdatensatzes (C_i , C_j , C_k); und
- 5 – Hinzufügen der Signatur zu dem quasi-maskierten elektronischen Münzdatensatz (Z_j , Z_j , Z_k) oder zu dem vollständig maskierten elektronischen Münzdatensatz oder dem teilbetragsmaskierten elektronischen Münzdatensatz,
- wobei in der Überwachungsinstanz (2) der vollständig maskierten elektronischen Münzdatensatz oder der teilbetragsmaskierte elektronische Münzdatensatz oder der
- 10 quasimaskierte elektronische Münzdatensatz mit der Signatur registriert wird.

11. Das Verfahren nach einem der Ansprüche 1 bis 10, mit den weiteren Verfahrensschritten:

- Erzeugen einer Signatur unter Verwendung des Verschleierungsbetrags (r_i , r_j , r_k) des elektronischen Münzdatensatzes (C_i , C_j , C_k); und
- 15 – Senden der Signatur zusammen mit dem quasi-maskierten elektronischen Münzdatensatz (Z_j , Z_j , Z_k) oder dem teilbetragsmaskierten elektronischen Münzdatensatz,
- wobei in der Überwachungsinstanz (2) nur der teilbetragsmaskierte elektronische Münzdatensatz oder der quasimaskierte elektronische Münzdatensatz registriert wird.

20 12. Das Verfahren nach einem der vorhergehenden Ansprüche, wobei die Überwachungsinstanz (2) nur teilbetragsmaskierte oder quasi-maskierte elektronische Münzdatensatz registriert; und/oder nur elektronische Münzdatensätze (C_i , C_j , C_k) registriert, die zumindest für einen Betragsanteil betragsoffen sind.

25 13. Das Verfahren nach einem der vorhergehenden Ansprüche mit den weiteren Verfahrensschritten:

- Umschalten des elektronischen Münzdatensatzes (C_i , C_j , C_k) unter Generieren eines umzuschaltenden elektronischen Münzdatensatzes (C_l), bevorzugt im ersten Endgerät (M1), aus dem elektronischen Münzdatensatzes (C_i , C_j , C_k), wobei ein Verschleierungsbetrag (r_l) für den umzuschaltenden elektronischen Münzdatensatz (C_l) unter Verwendung des Verschleierungsbetrags (r_i , r_j , r_k) des elektronischen Münzdatensatzes (C_i , C_j , C_k), bevorzugt im ersten Endgerät (M1), erzeugt wird; und der monetäre Betrag (v_i , v_j , v_k) des elektronischen Münzdatensatzes (C_i , C_j , C_k) als ein monetärer Betrag (v_l) für den umzuschaltenden elektronischen Münzdatensatz (C_l) verwendet wird; und/ oder
- 30 – Aufteilen des elektronischen Münzdatensatzes (C_j) in einen ersten elektronischen Münzteildatensatz (C_j) und einen zweiten elektronischen Münzteildatensatz (C_k),
- 35

bevorzugt im ersten Endgerät (M1), wobei der monetäre Betrag (v_i) in wenigstens einen ersten monetären Betrag (v_j) und einen zweiten monetären Betrag (v_k) aufgeteilt wird; und/oder

- Verbinden eines ersten und eines zweiten elektronischen Münzdatensatzes (C_i , C_j) zu einem verbundenen elektronischen Münzdatensatzes (C_m) im ersten Endgerät (M1) mit den Schritten:
 - Berechnen eines Verschleierungsbetrags (r_m) für den zu verbindenden elektronischen Münzdatensatz (C_m) durch Bilden der Summe aus den jeweiligen Verschleierungsbeträgen des ersten und des zweiten elektronischen Münzdatensatzes (r_i , r_j); und
 - Berechnen des monetären Betrags (v_m) für den zu verbindenden elektronischen Münzdatensatz (C_m) durch Bilden der Summe aus den jeweiligen monetären Beträgen (v_i , v_j) des ersten und des zweiten elektronischen Münzdatensatzes (C_i , C_j);
- wobei das Maskieren des elektronischen Münzdatensatzes (C_i , C_j , C_k) im Maskieren-Schritt des ersten, zweiten oder dritten Maskierungsmodus das Maskieren des umzuschaltenden Münzdatensatzes (C_l), des ersten und/oder zweiten Münzteildatensatzes (C_j , C_k) und/oder des verbundenen Münzdatensatzes (C_m) umfasst oder wobei das Maskieren des Datensatzelementes, bevorzugt des Verschleierungsbetrags (r_i , r_j , r_k), des elektronischen Münzdatensatzes, das Maskieren des Datensatzelementes, bevorzugt des Verschleierungsbetrags (r_l), des umzuschaltenden Münzdatensatzes (C_l), des Datensatzelementes, bevorzugt des Verschleierungsbetrags (r_j), des ersten und/oder des Datensatzelementes, bevorzugt des Verschleierungsbetrags (r_k), des zweiten Münzteildatensatzes (C_j , C_k) und/oder des Datensatzelementes, bevorzugt des Verschleierungsbetrags (r_m), des verbundenen Münzdatensatzes (C_m) umfasst, und
- Senden des vollständig maskierten elektronischen Münzdatensatzes (Z_j , Z_j , Z_k , Z_l , Z_m) oder des quasimaskierten elektronischen Münzdatensatzes oder des teilbetragsmaskierten elektronischen Münzdatensatzes an die Überwachungsinstanz (2), bevorzugt vom ersten Endgerät (M1), an die Überwachungsinstanz (2) zum Prüfen (107) der Validität des elektronischen Münzdatensatzes (C_i , C_j , C_k , C_l , C_m) durch die Überwachungsinstanz (2).

14. Das Verfahren nach Anspruch 13, wobei nach dem Schritt des Umschaltens der Registrieren-Schritt in der Überwachungsinstanz (2) für den ersten Maskierungsmodus umfasst:

- Empfangen des quasi-maskierten umzuschaltenden elektronischen Münzdatensatzes (Z_l) in der Überwachungsinstanz (2);
- Prüfen des quasi-maskierten elektronischen Münzdatensatzes auf Validität in der Überwachungsinstanz (2);

- Prüfen einer, dem quasi-maskierten elektronischen Münzdatensatz hinzugefügten Signatur unter Verwendung des verschlüsselten Verschleierungsbetrags (R_i , R_j , R_k) des elektronischen Münzdatensatzes (C_i , C_j , C_k) in der Überwachungsinstanz (2); und
- Registrieren des quasi-maskierten umzuschaltenden elektronischen Münzdatensatzes in der Überwachungsinstanz (2), wenn die beiden Prüfen-Schritte erfolgreich sind, wodurch der umzuschaltende elektronische Münzdatensatz (C_l) als gültig gilt.

15. Das Verfahren nach Anspruch 13, wobei nach dem Schritt des Aufteilens der Registrieren-Schritt in der Überwachungsinstanz (2) für den ersten Maskierungsmodus umfasst:

- Empfangen der quasi-maskierten elektronischen Münzteildatensätze in der Überwachungsinstanz (2);
- Prüfen des quasi-maskierten elektronischen Münzdatensatzes auf Validität in der Überwachungsinstanz;
- Prüfen einer, den quasi-maskierten elektronischen Münzteildatensätzen hinzugefügten Signatur unter Verwendung des maskierten Verschleierungsbetrags (R_i) in der Überwachungsinstanz (2);
- Prüfen, ob der monetäre Betrag (v_i) des elektronischen Münzdatensatzes (C_i) gleich der Summe aus ersten und zweiten monetären Betrag (v_j , v_k) der elektronischen Münzteildatensätze (C_j , C_k) ist;
- Registrieren der quasi-maskierten elektronischen Münzteildatensätze in der Überwachungsinstanz (2), wenn die drei Prüfen-Schritte erfolgreich sind, wodurch die elektronischen Münzteildatensätze (C_j , C_k) als gültig gelten und der aufzuteilende elektronische Münzdatensatz als ungültig.

16. Das Verfahren nach Anspruch 13, wobei nach dem Schritt des Verbindens der Registrieren-Schritt in der Überwachungsinstanz (2) für den ersten Maskierungsmodus umfasst:

- Empfangen des quasi-maskierten verbundenen elektronischen Münzdatensatzes in der Überwachungsinstanz (2);
- Prüfen der quasi-maskierten ersten und zweiten elektronischen Münzdatensätze auf Validität in der Überwachungsinstanz (2);
- Prüfen zweier, den zu verbindenden quasi-maskierten verbundenen elektronischen Münzdatensätzen hinzugefügten Signaturen unter Verwendung der jeweiligen maskierten Münzdatensatzelemente, bevorzugt der maskierten Verschleierungsbeträge (R_j) in der Überwachungsinstanz (2);
- Prüfen, ob der monetäre Betrag (v_m) des verbundenen elektronischen Münzdatensatzes (C_m) gleich der Summe aus dem ersten und dem zweiten monetären Betrag (v_i , v_j) der ersten und zweiten elektronischen Münzdatensätze (C_i , C_j) ist;

- Registrieren des quasi-maskierten verbundenen elektronischen Münzdatensatzes in der Überwachungsinstanz (2) wenn die drei Prüfen-Schritte erfolgreich sind, wodurch der verbundene elektronische Münzdatensatz (C_m) als gültig gilt und die zwei zu verbindenden elektronischen Münzdatensätze als ungültig.

5

17. Das Verfahren nach einem der Ansprüche 10 bis 16, wobei die hinzugefügte Signatur eine erste Signatur ist und ein privater Signaturschlüssel zum Erzeugen der ersten Signatur der Verschleierungsbetrag (r_i , r_j , r_k) des elektronischen Münzdatensatzes (C_i , C_j , C_k) ist.

10 18. Das Verfahren nach einem der Ansprüche 10 bis 18, wobei die hinzugefügte Signatur eine zweite Signatur ist und ein privater Signaturschlüssel zum Erzeugen der zweiten Signatur aus einer Differenz aus dem Verschleierungsbetrag (r_i , r_j , r_k) des elektronischen Münzdatensatzes (C_i , C_j , C_k) und dem Verschleierungsbetrag (r_i) für den umzuschaltenden elektronischen Münzdatensatz (C_i) gebildet wird.

15

19. Das Verfahren nach einem der Ansprüche 16 oder 17, wobei ein öffentlicher Verifikationsschlüssel zum Prüfen der ersten Signatur aus einer Differenz aus dem maskierten elektronischen Münzdatensatz (Z_i) und einem Anwenden der kryptografischen Verschlüsselungsfunktion auf den monetären Betrag (r_i , r_j , r_k) des elektronischen Münzdatensatzes (C_i , C_j , C_k) gebildet wird.

20

20. Das Verfahren nach einem der Ansprüche 16 oder 17, wobei ein öffentlicher Verifikationsschlüssel zum Prüfen der zweiten Signatur aus einer Differenz aus dem unvollständig maskierten elektronischen Münzdatensatz (Z_i) und dem maskierten elektronischen Münzdatensatz (Z_i) gebildet wird.

25

21. Das Verfahren nach einem der vorhergehenden Ansprüche, wobei der zumindest eine elektronische Münzdatensatzes (C_i , C_j , C_k) von einer Herausgeberinstanz (1) erzeugt wurde, wobei die Herausgeberinstanz (1) einen vollständig maskierten oder teilbetragsmaskierten oder quasi-maskierten elektronischen Münzdatensatz mit ihrer Signatur ($[Z_i]Sig_i$) signiert und wobei diese Signatur ($[Z_i]Sig_i$) in der Überwachungsinstanz (2) hinterlegt wird.

30

22. Ein Bezahlssystem zum Austausch von monetären Beträgen, wobei das Bezahlssystem umfasst:

35

- eine Überwachungsschicht (4) mit einer Datenbank in der vollständig maskierte elektronische Münzdatensätze oder teilbetragsmaskierte elektronische Münzdatensätze oder quasi-maskierte elektronische Münzdatensätze abgelegt sind; und

- eine Direkttransaktionsschicht (3) mit zumindest zwei Endgeräten (M1, M2, M3), in welcher das Verfahren (100) nach einem der vorhergehenden Ansprüche 1 bis 21 durchführbar ist; und/oder einer Herausgeberinstanz (1) zum Erzeugen eines elektronischen Münzdatensatzes (C_i , C_j , C_k) und bevorzugt einer Signatur ($[Z_i]Sig_i$), wobei die Signatur ($[Z_i]Sig_i$) in der Datenbank hinterlegt ist.

23. Währungssystem, umfassend eine Herausgeberinstanz (1), eine Überwachungsinstanz (2), ein erstes Endgerät (M1) und ein zweites Endgerät (M2, M3), wobei eine Herausgeberinstanz ausgebildet ist, einen elektronischen Münzdatensatzes (C_i) zu erstellen, wobei ein vollständig maskierter elektronische Münzdatensatz oder ein teilbetragsmaskierter elektronischer Münzdatensatz oder ein quasi-maskierter elektronischer Münzdatensatz ausgebildet ist, nachweisbar durch die Herausgeberinstanz (1) erstellt zu sein, wobei die Überwachungsinstanz (2) zum Ausführen eines Registrierschritts nach einem der Ansprüche 1 bis 21 ausgebildet ist.

24. Währungssystem nach Anspruch 23, wobei das erste und zweite Endgerät (M1, M2, M3) zum Durchführen eines Verfahrens nach einem der Ansprüche 1 bis 21 ausgebildet sind.

25. Währungssystem nach einen der Ansprüche 23 oder 24, wobei die Überprüfungsinstanz (2) und die Herausgeberinstanz (1) als Serverinstanz, insbesondere als Computerprogrammprodukt auf einem Server und/ oder einem Computer implementiert sind.

26. Währungssystem nach einem der Ansprüche 23 bis 25, wobei das erste und/ oder zweite Endgerät (M1, M2, M3) als mobiles Endgerät, insbesondere als ein Smartphone, ein Tablet-Computer, ein Computer, ein Server oder eine Maschine, und/ oder als passives Endgerät, insbesondere Smart Card oder als Wearable, ausgebildet sind.

27. Überwachungseinheit (4) eingerichtet zum:

Empfangen eines maskierten elektronischen Münzdatensatzes (Z_j , Z_j , Z_k); und

Registrieren des maskierten elektronischen Münzdatensatzes (Z_j , Z_j , Z_k),

wobei der maskierte elektronische Münzdatensatz (Z_j , Z_j , Z_k) in einem erstem Maskierungsmodus oder einem zweiten Maskierungsmodus, bevorzugt gemäß Maskierungsschritten aus dem Verfahren nach einem der vorhergehenden Ansprüche 1 bis 21, maskiert ist.

1/13

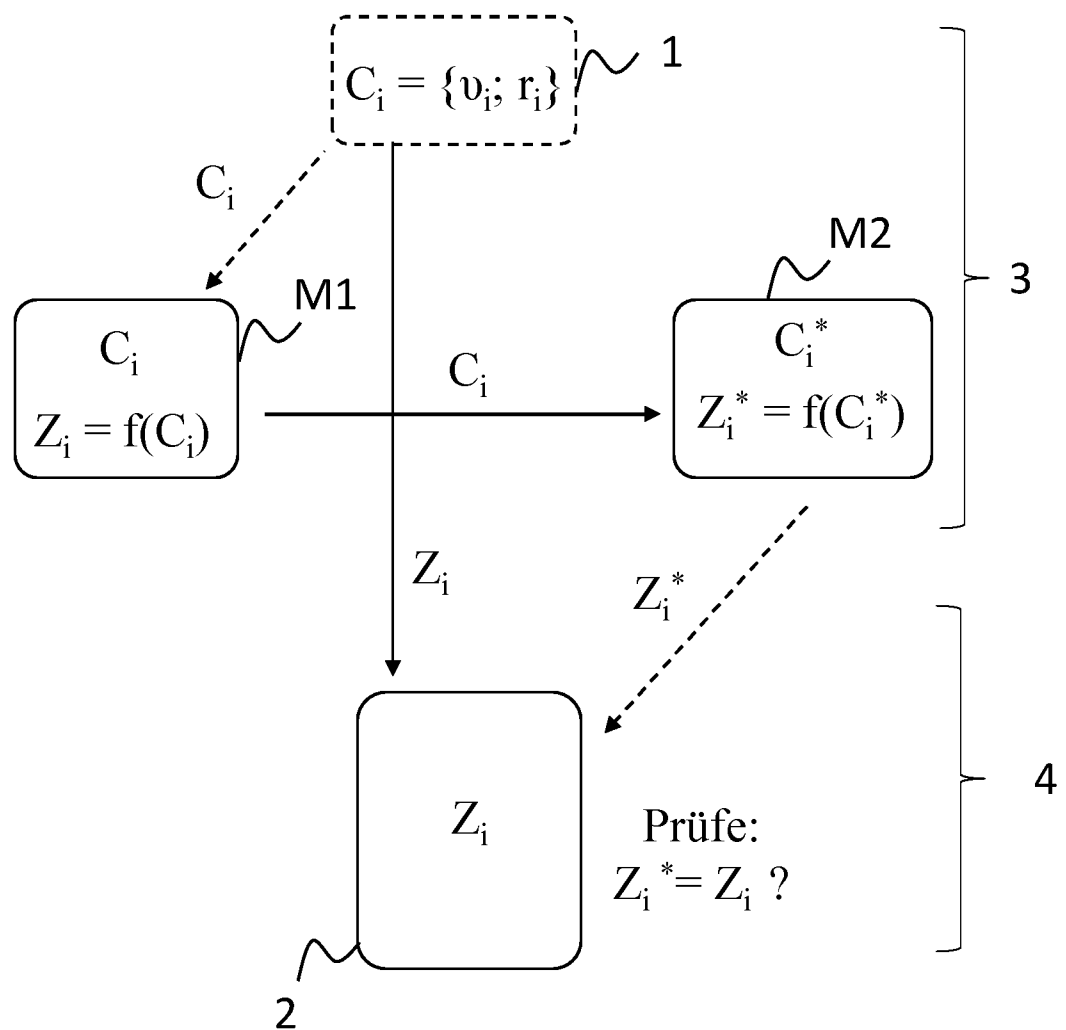


Fig. 1

2/13

	21	22a	22b	23a	23b	24	25	26	27	28
Kommando	O_1	O_2	S_1	S_2	Signatur	O-Flag	C-Flag	R-Flag	S-Flag	
Erzeugen	-	-	Z_i	-	$[Z_i]Sig_i$	-	-	-	$[0,1]$	
Deaktivieren	Z_i	-	-	-	$[Z_i]Sig_i$	$[0,1]$	-	-	$[0,1]$	
Aufteilen	Z_i	-	Z_j	Z_k	Sig	$[0,1]$	$[0,1]$	$[0,1]$	-	
Verbinden	Z_i	Z_j	-	Z_m	$Sig\ 1,2$	$[0,1]$	$[0,1]$	$[0,1]$	-	
Umschalten	Z_k	-	-	Z_l	Sig	$[0,1]$	$[0,1]$	$[0,1]$	-	

2

Fig. 2

3/13

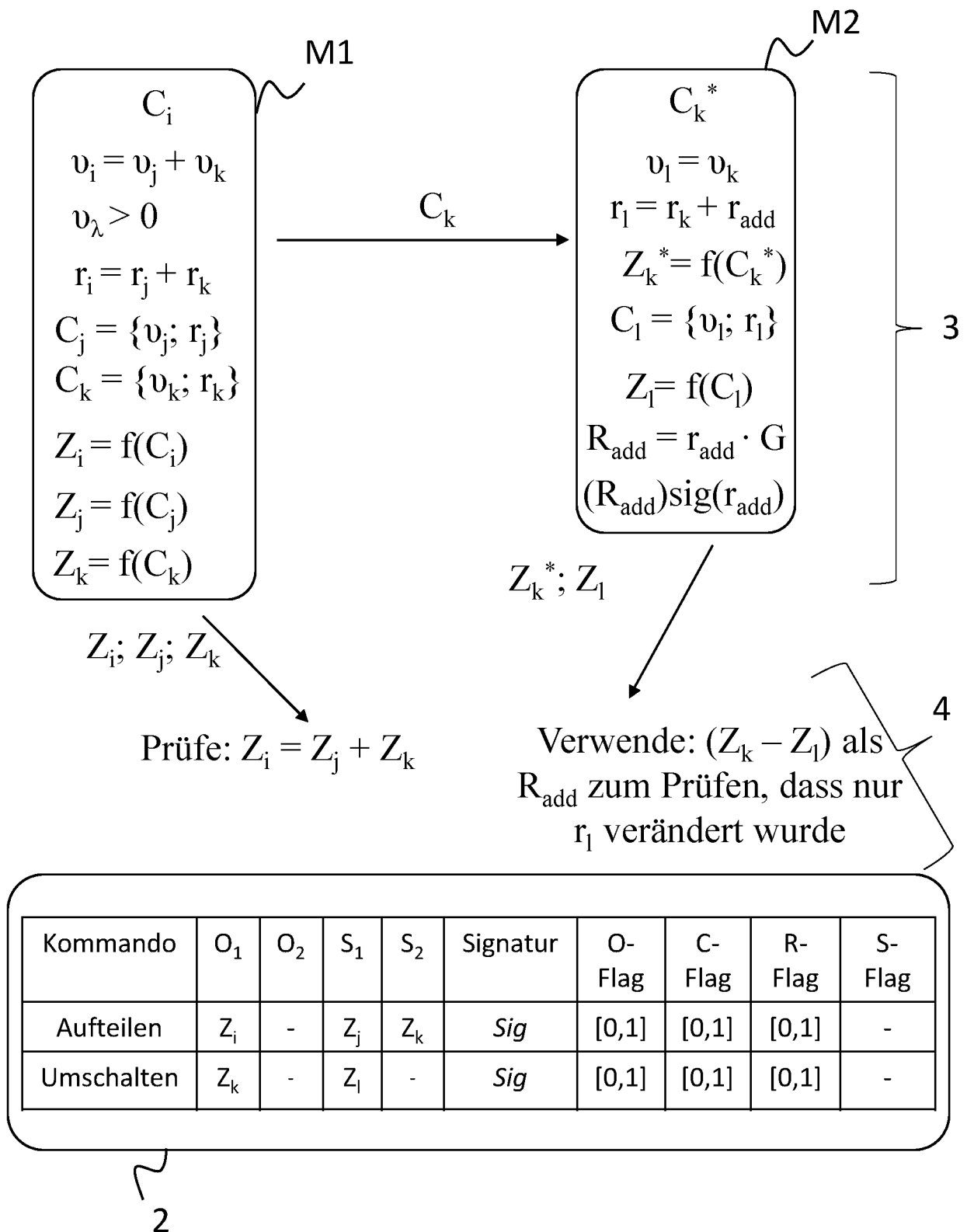


Fig. 3

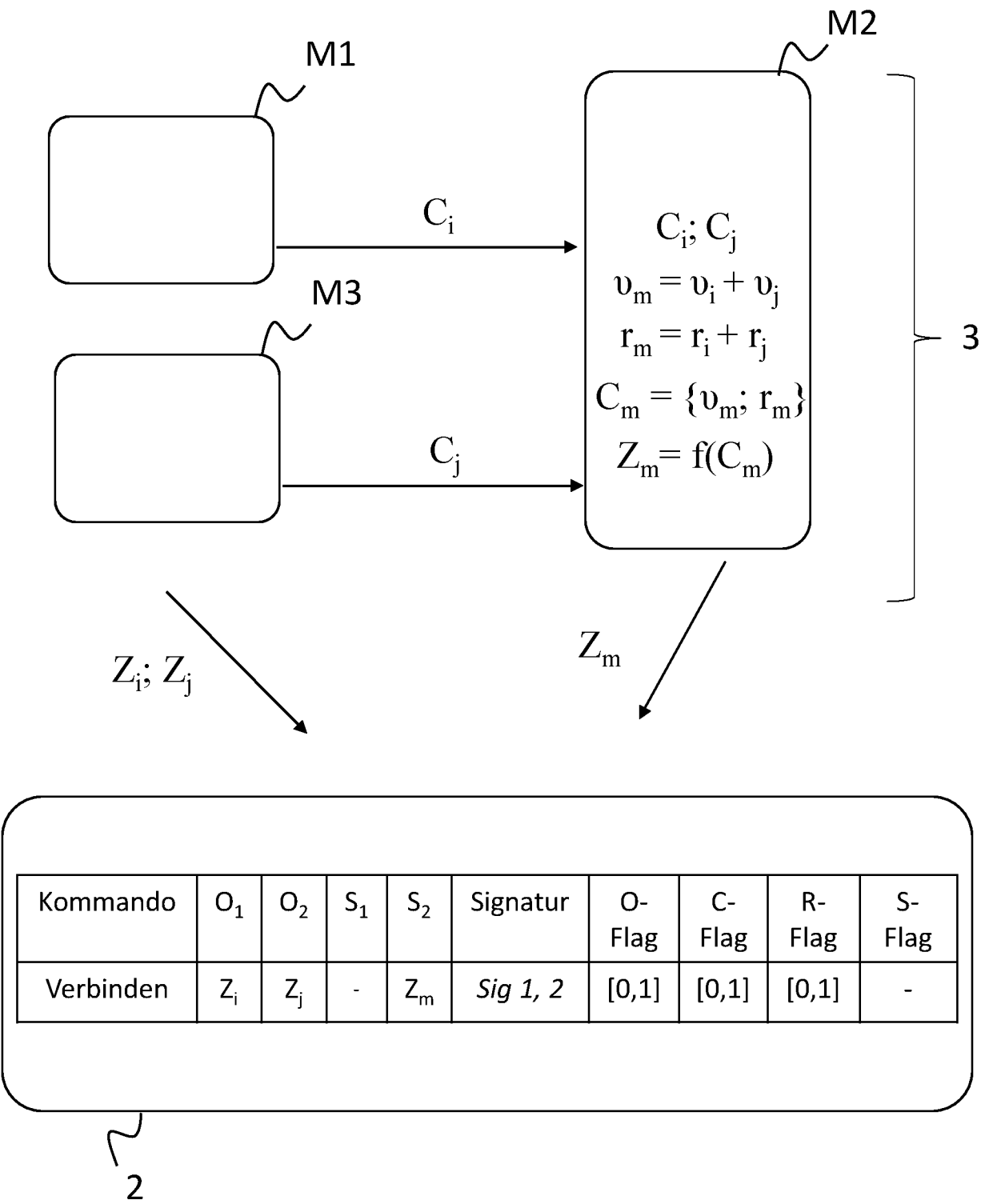


Fig. 4

5/13

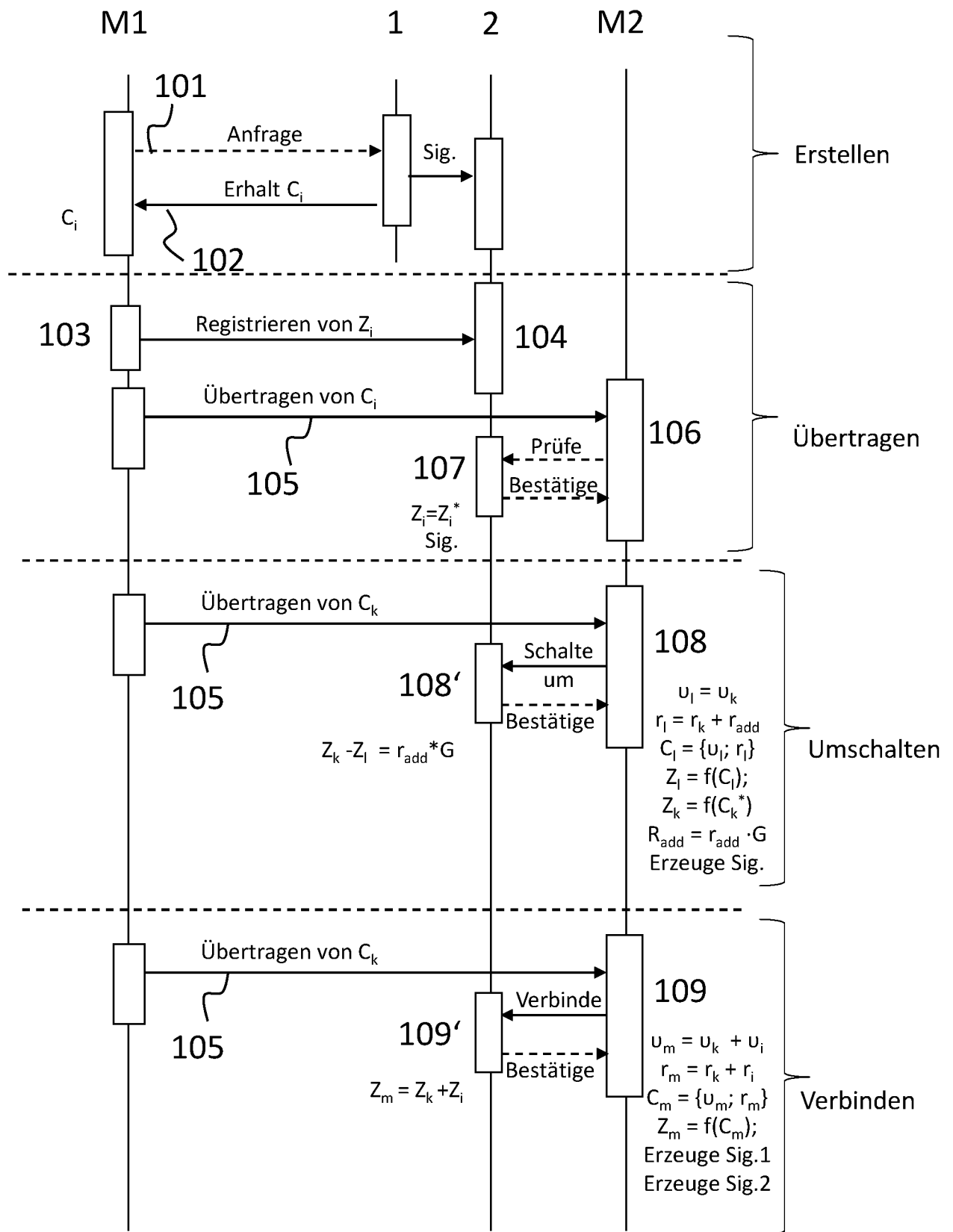


Fig. 5

6/13

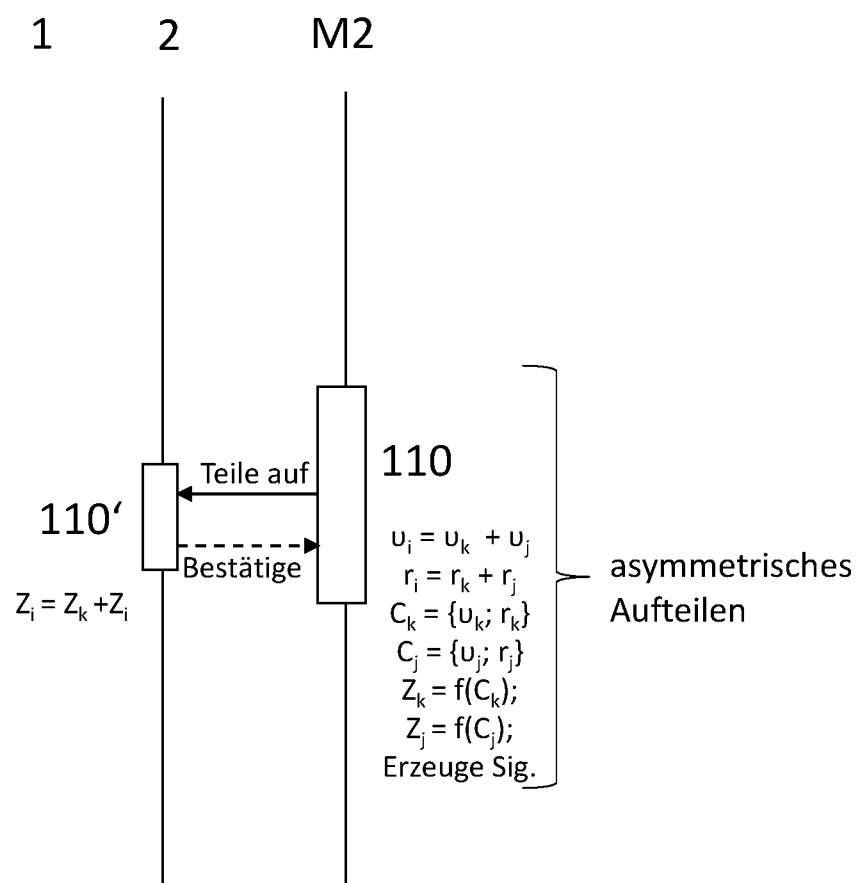
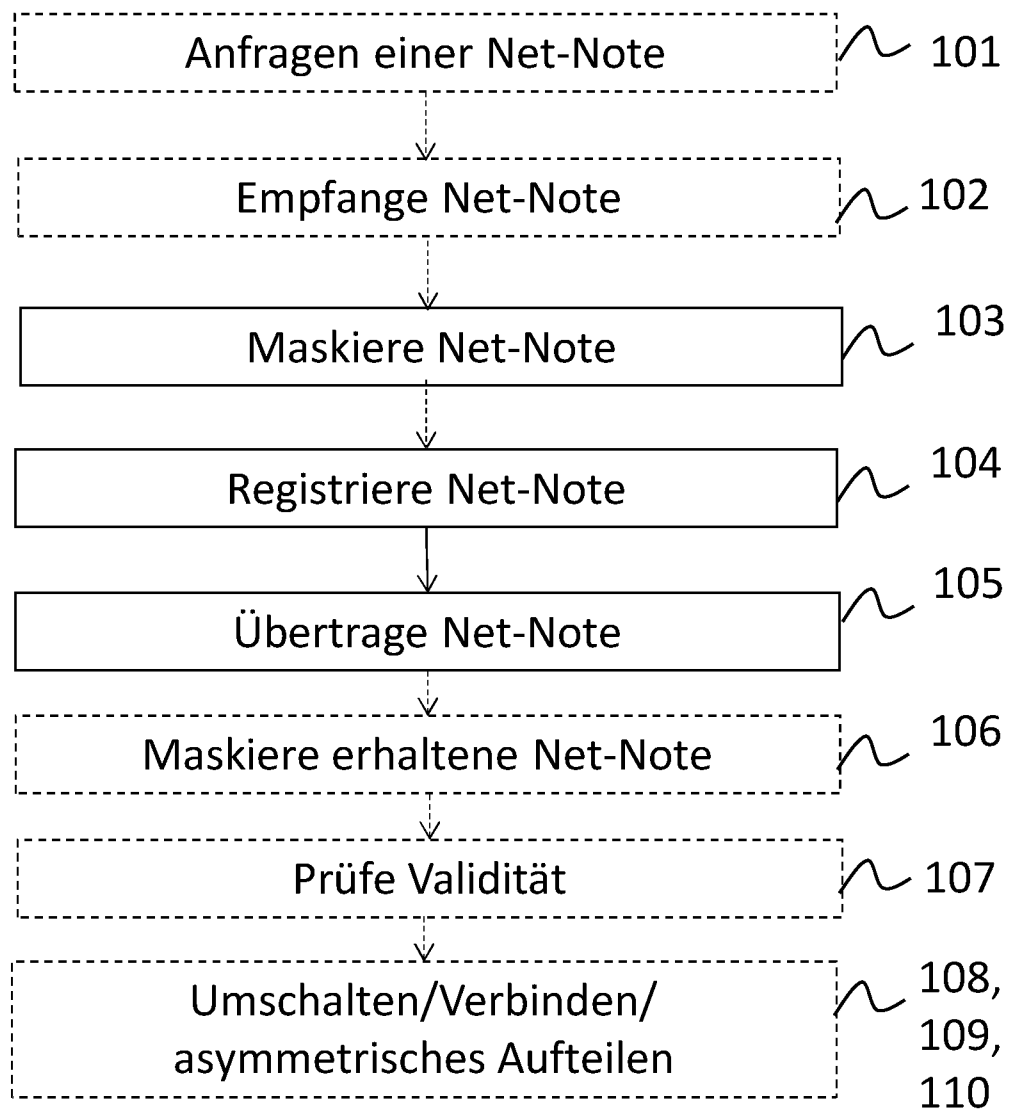


Fig. 6

7/13

100**Fig. 7**

8/13

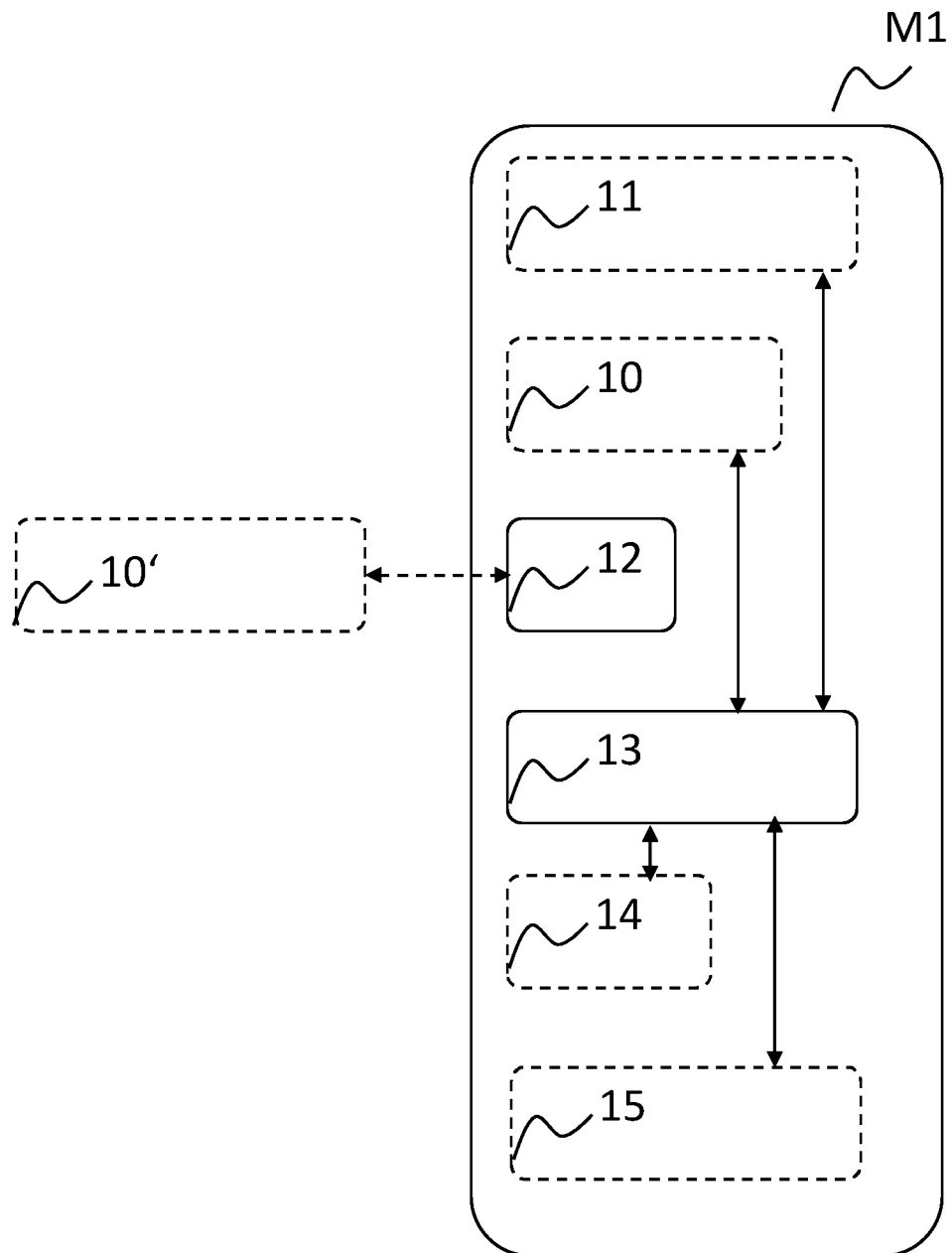


Fig. 8

9/13

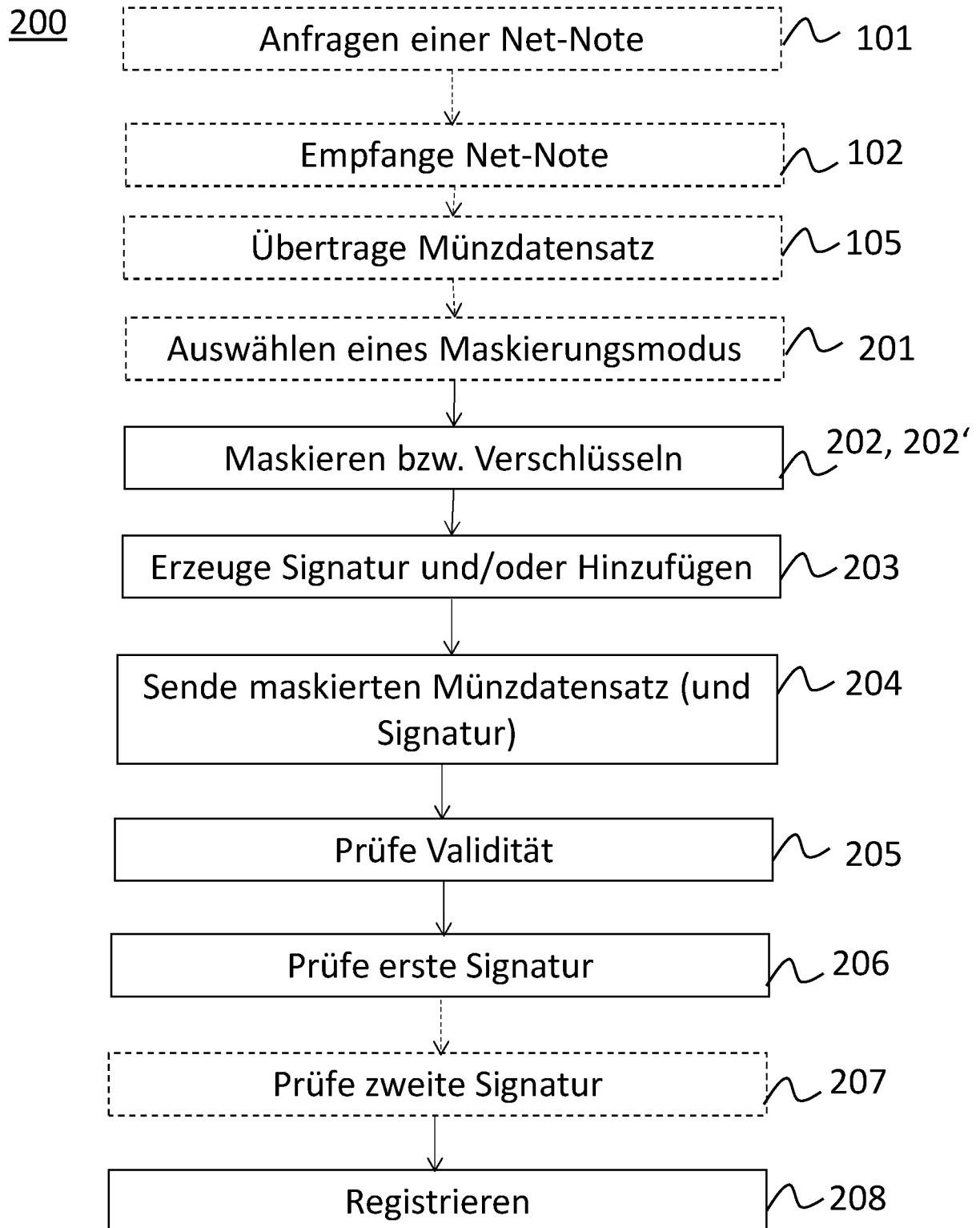


Fig. 9

10/13

200

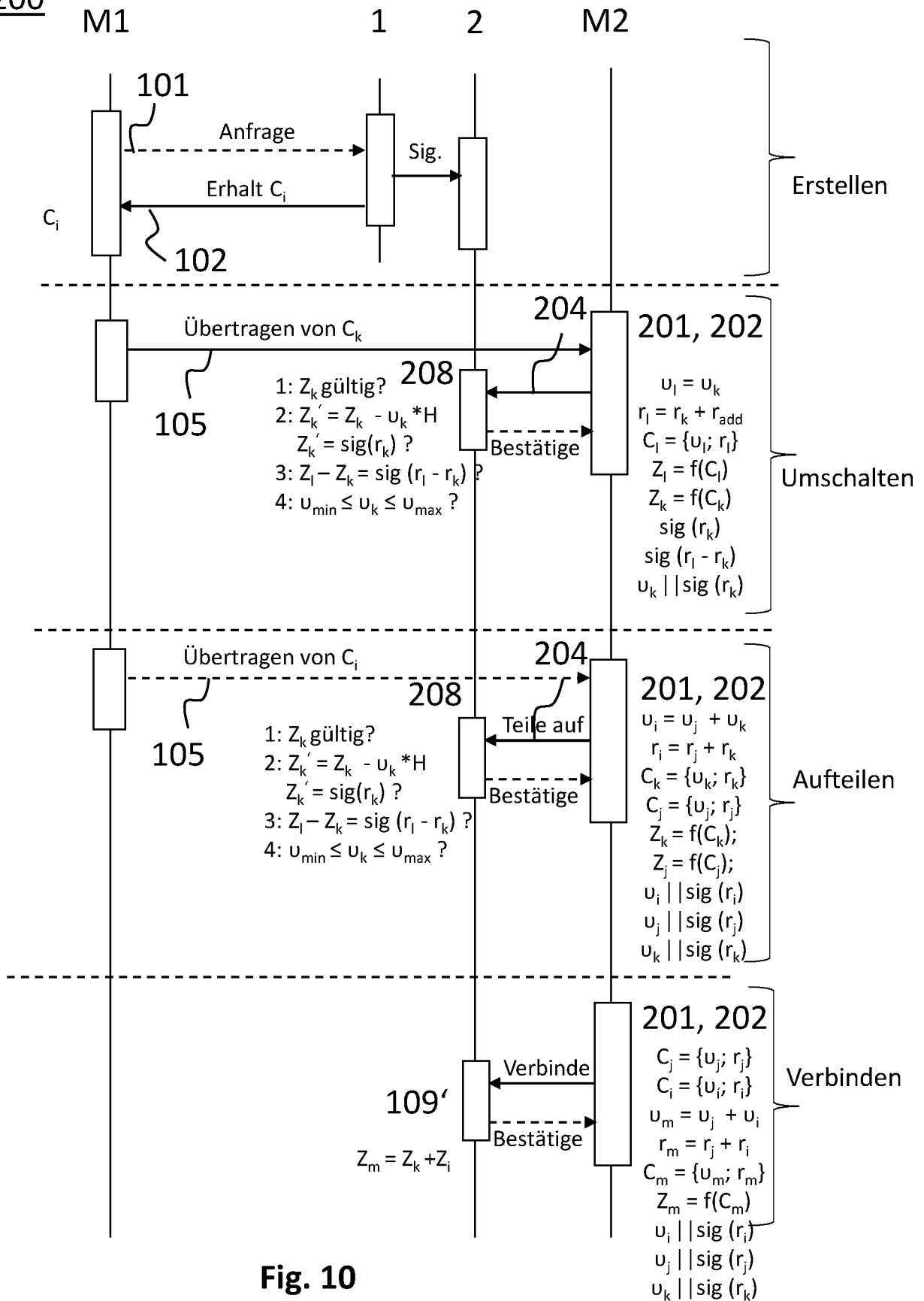


Fig. 10

11/13

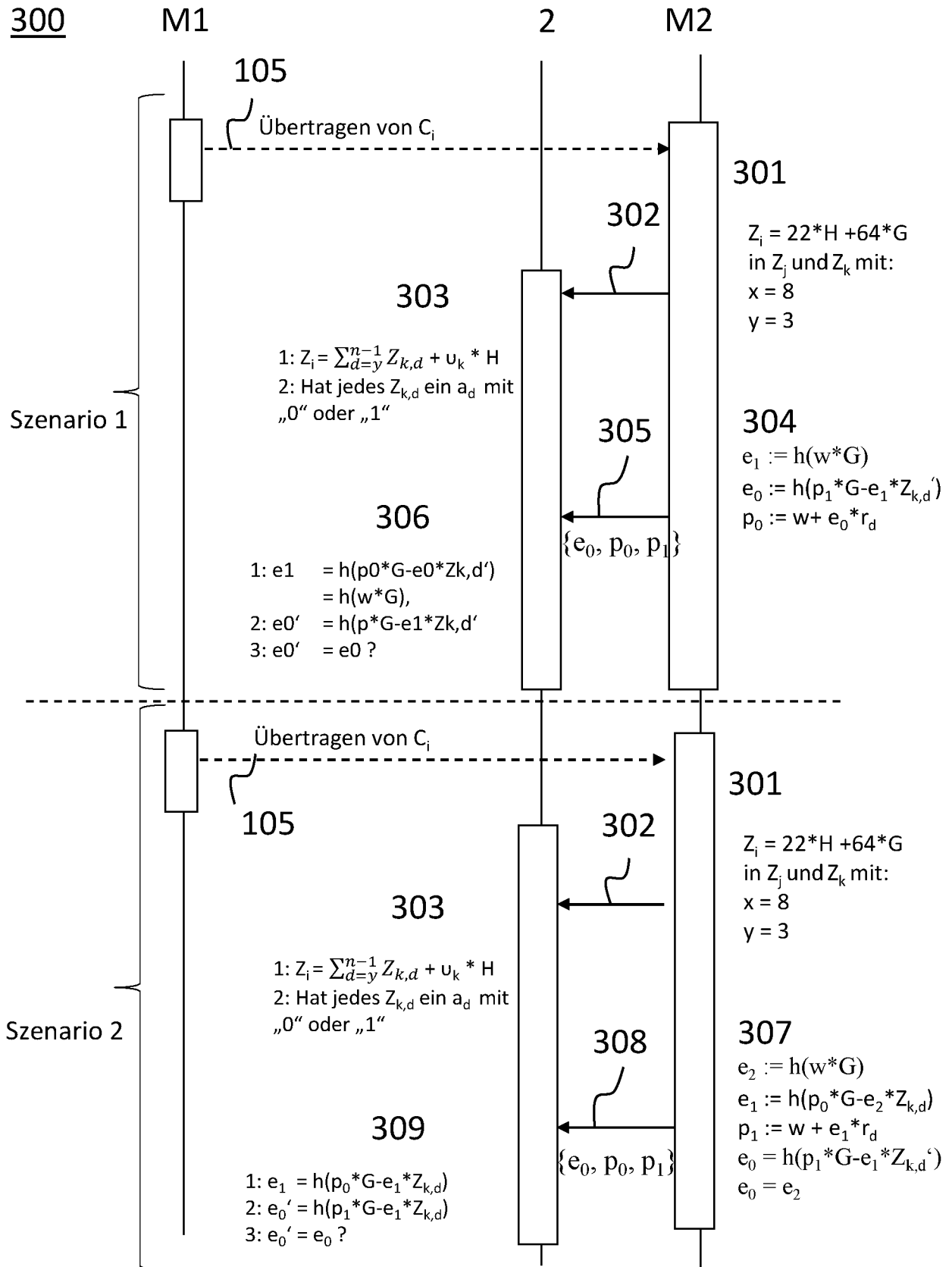
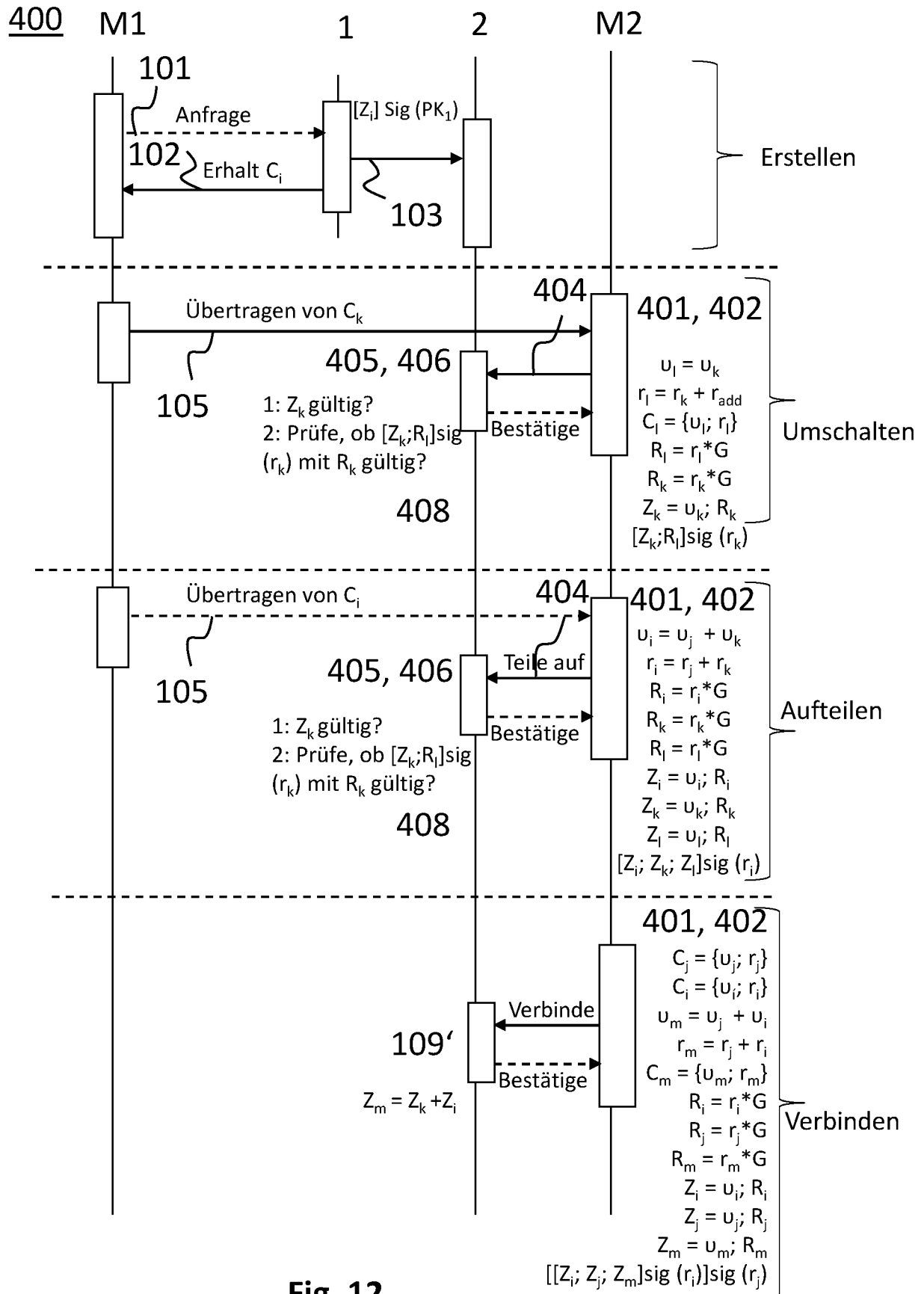
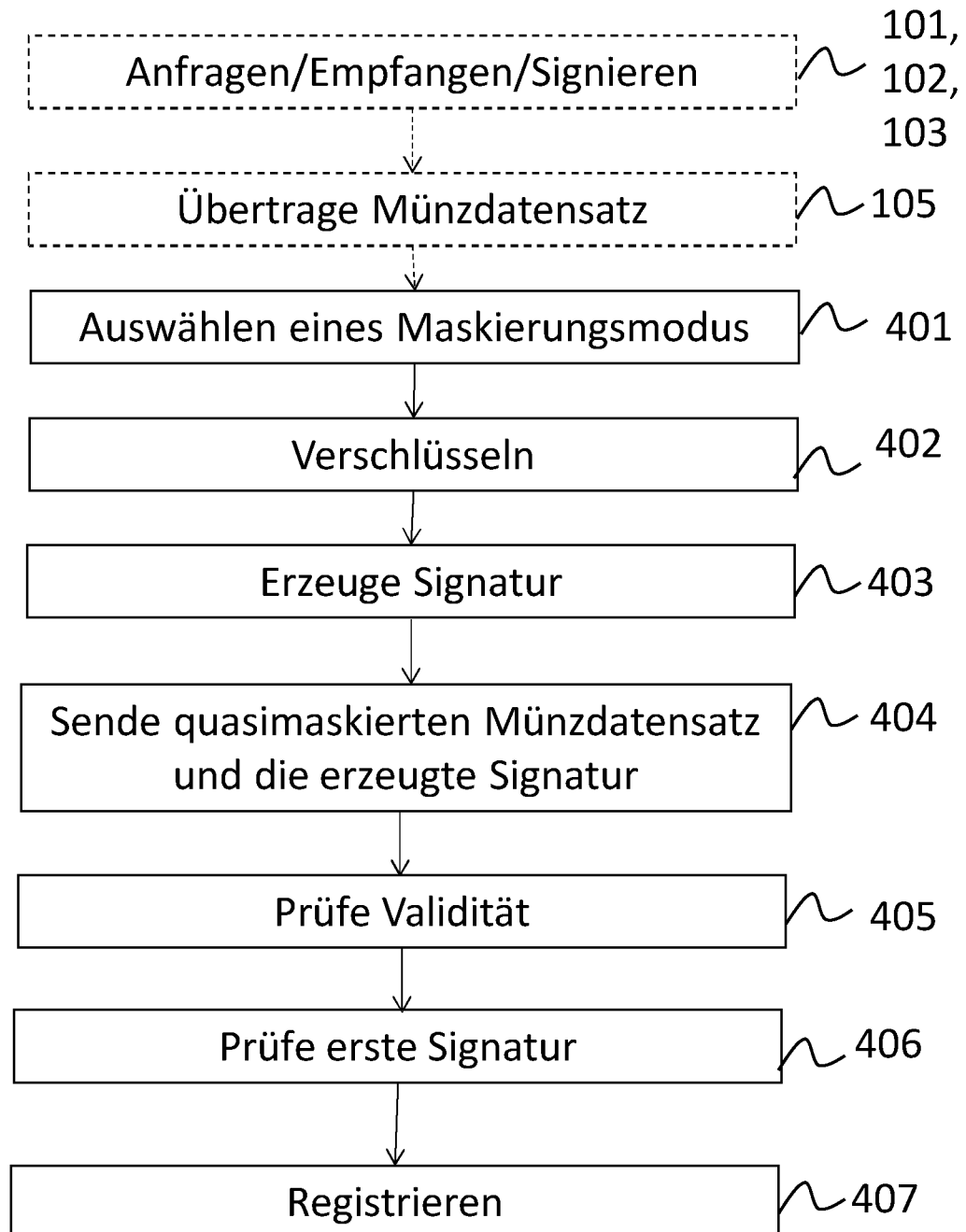


Fig. 11

12/13



13/13

400**Fig. 13**

INTERNATIONAL SEARCH REPORT

International application No.

PCT/EP2021/054543

A. CLASSIFICATION OF SUBJECT MATTER**G06F 21/64**(2013.01)i; **G06Q 20/06**(2012.01)i; **G06Q 20/36**(2012.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F; G07G; G06Q

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	US 2016358165 A1 (MAXWELL GREGORY [US]) 08 December 2016 (2016-12-08) abstract paragraph [0018] - paragraph [0022]	1-4,22,23,27 5-21,24-26
A	EP 3549082 A2 (ALIBABA GROUP HOLDING LTD [KY]) 09 October 2019 (2019-10-09) abstract	1-27
A	ISABELLE SIMPLOT-RYL ET AL. "Distributed architectures for electronic cash schemes: a survey1" <i>INTERNATIONAL JOURNAL OF PARALLEL, EMERGENT AND DISTRIBUTED SYSTEMS</i> , United Kingdom, Vol. 24, No. 3, 01 June 2009 (2009-06-01), pages 243-271 DOI: 10.1080/17445760802441671 ISSN: 1744-5760, XP055672436 paragraph [04.1] paragraph [04.3]	1-27



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search

14 May 2021

Date of mailing of the international search report

25 May 2021

Name and mailing address of the ISA/EP

European Patent Office
p.b. 5818, Patentlaan 2, 2280 HV Rijswijk
Netherlands

Telephone No. (+31-70)340-2040

Facsimile No. (+31-70)340-3016

Authorized officer

Meződi, Stephan

Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.

PCT/EP2021/054543

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
US	2016358165	A1	08 December 2016	US	2016358165	A1	08 December 2016
				WO	2016200885	A1	15 December 2016
EP	3549082	A2	09 October 2019	AU	2018347196	B2	14 May 2020
				BR	112019007907	A2	12 November 2019
				CA	3040611	A1	18 April 2019
				CN	110419053	A	05 November 2019
				EP	3549082	A2	09 October 2019
				EP	3745637	A1	02 December 2020
				JP	2020502856	A	23 January 2020
				KR	20200066259	A	09 June 2020
				PH	12019500860	A1	02 December 2019
				SG	11201903438T	A	30 May 2019
				US	2020058022	A1	20 February 2020
				US	2020111093	A1	09 April 2020
				WO	2019072278	A2	18 April 2019
				ZA	201902472	B	26 August 2020

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES INV. G06F21/64 G06Q20/06 G06Q20/36 ADD.		
Nach der Internationalen Patentklassifikation (IPC) oder nach der nationalen Klassifikation und der IPC		
B. RECHERCHIERTE GEBIETE Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole) G06F G07G G06Q		
Recherchierte, aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen		
Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe) EPO-Internal		
C. ALS WESENTLICH ANGESEHENE UNTERLAGEN		
Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 2016/358165 A1 (MAXWELL GREGORY [US]) 8. Dezember 2016 (2016-12-08)	1-4,22, 23,27
A	Zusammenfassung Absatz [0018] - Absatz [0022]	5-21, 24-26
A	EP 3 549 082 A2 (ALIBABA GROUP HOLDING LTD [KY]) 9. Oktober 2019 (2019-10-09) Zusammenfassung ----- -/-	1-27
☒ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen ☒ Siehe Anhang Patentfamilie		
* Besondere Kategorien von angegebenen Veröffentlichungen : "A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist "E" frühere Anmeldung oder Patent, die bzw. das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist "L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt) "O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht "P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist "T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist "X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden "Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist "&" Veröffentlichung, die Mitglied derselben Patentfamilie ist		
Datum des Abschlusses der internationalen Recherche		Absendedatum des internationalen Recherchenberichts
14. Mai 2021		25/05/2021
Name und Postanschrift der Internationalen Recherchenbehörde Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016		Bevollmächtigter Bediensteter Mezödi, Stephan

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN		
Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	ISABELLE SIMPLOT-RYL ET AL: "Distributed architectures for electronic cash schemes: a survey1", INTERNATIONAL JOURNAL OF PARALLEL, EMERGENT AND DISTRIBUTED SYSTEMS, Bd. 24, Nr. 3, 1. Juni 2009 (2009-06-01), Seiten 243-271, XP055672436, United Kingdom ISSN: 1744-5760, DOI: 10.1080/17445760802441671 Absatz [04.1] Absatz [04.3] -----	1-27

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP2021/054543

Im Recherchenbericht angeführtes Patentdokument			Datum der Veröffentlichung		Mitglied(er) der Patentfamilie		Datum der Veröffentlichung	
US	2016358165	A1	08-12-2016	US	2016358165	A1	08-12-2016	
				WO	2016200885	A1	15-12-2016	

EP	3549082	A2	09-10-2019	AU	2018347196	B2	14-05-2020	
				BR	112019007907	A2	12-11-2019	
				CA	3040611	A1	18-04-2019	
				CN	110419053	A	05-11-2019	
				EP	3549082	A2	09-10-2019	
				EP	3745637	A1	02-12-2020	
				JP	2020502856	A	23-01-2020	
				KR	20200066259	A	09-06-2020	
				PH	12019500860	A1	02-12-2019	
				SG	11201903438T	A	30-05-2019	
				US	2020058022	A1	20-02-2020	
				US	2020111093	A1	09-04-2020	
				WO	2019072278	A2	18-04-2019	
				ZA	201902472	B	26-08-2020	
