(19) Deutsches Patent- und Markenamt

(10) **DE 20 2018 102 306 U1** 2018.10.04

(12) # Gebrauchsmusterschrift

(21) Aktenzeichen: **20 2018 102 306.3**
(22) Anmeldetag: **04.04.2018**
(67) aus Patentanmeldung: **PCT/US2018/026136**
(47) Eintragungstag: **28.08.2018**
(45) Bekanntmachungstag im Patentblatt: **04.10.2018**

(51) Int Cl.: ***G06Q 20/36*** (2012.01)
G06F 21/00 (2013.01)
G06F 21/31 (2013.01)
G06Q 20/38 (2012.01)

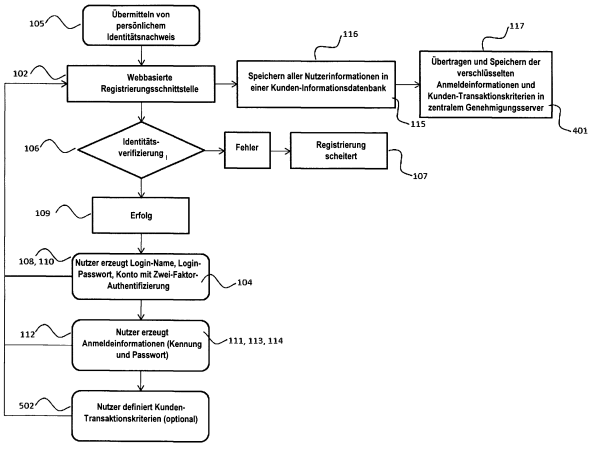
(73) Name und Wohnsitz des Inhabers:
BLACK GOLD COIN, INC., Las Vegas, Nev., US

(74) Name und Wohnsitz des Vertreters:
BOEHMERT & BOEHMERT Anwaltspartnerschaft mbB - Patentanwälte Rechtsanwälte, 80336 München, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen.

(54) Bezeichnung: **Systeme zur persönlichen Identifizierung und Verifizierung**

(57) Hauptanspruch: System zum Überwachen und Beschränken von Transaktionen mit Kryptographie-basiertem elektronischem Geld (CBEM), wobei das System umfasst:
einen Systemprozessor (420 und/oder 707), der ein Systemverwaltungsdienstprogramm ausführt, das zum Verarbeiten von Kunden-Identitätsregistrierungen, Kunden-Währungsadressen und CBEM-Transaktionen eingerichtet ist zum:
- Kommunizieren mit einem Kunden-Wallet (416, 417), um eine oder mehrere genehmigte Währungsadressen des Kunden zu erzeugen;
- Genehmigen einer Anfrage zur Erzeugung einer oder mehrerer genehmigter Währungsadressen des Kunden;
- Kommunizieren mit dem Kunden-Wallet (416, 417), um eine oder mehrere genehmigte Transaktionen zu erzeugen;
- Genehmigen einer oder mehrerer Transaktionen, um eine Einheit des CBEM an eine Währungsadresse zu senden;
- Untersuchen einer Transaktion unter Verwendung von Transaktionskriterien, die von einem zentralen Leitungsorgan oder einem Kunden definiert werden; und
- Speichern von Transaktionsinformationen (414) in einer Transaktionsdatenbank (413);
wobei das System ferner umfasst:
eine oder mehrere genehmigte Währungsadressen;
ein genehmigtes Transaktionsnetzwerk;
eine Kunden-Informationsdatenbank (115), die kommunikativ mit dem Systemprozessor (420 und/oder 707) verbunden ist;
eine Transaktionsdatenbank (413), die kommunikativ mit dem Systemprozessor (420 und/oder 707) verbunden ist; und
mindestens ein Kunden-Gerät (414, 415), das mit einem Kunden-Wallet (416, 417) versehen ist;
wobei ...



Beschreibung

GEBIET DER OFFENBARUNG

[0001] Die vorliegende Erfindung betrifft ein System zur persönlichen Identifizierung und Verifizierung. Insbesondere bezieht sich die vorliegende Erfindung auf ein System zur Personen/Kunden-Identifizierung und -Verifizierung, ein pseudonymes System und ein Transaktionsnetzwerk zum Überwachen und Beschränken von Transaktionen eines Anmeldeinformations-Authentifizierungsprotokolls mit Verknüpfung von Kryptographie-basiertem elektronischem Geld und rechtlicher Identität.

HINTERGRUND

[0002] Der Stand der Technik definiert digitale Währung oder digitales Geld. Es ist ein internetbasiertes Tauschmittel (d. h. es unterscheidet sich von einem physischen wie Banknoten und Münzen), das ähnliche Eigenschaften wie physische Währungen aufweist, jedoch sofortige Transaktionen und grenzenlose Eigentumsübertragung erlaubt.

[0003] Sowohl virtuelle Währungen als auch Kryptowährungen sind Arten digitaler Währung, aber umgekehrt gilt das nicht. Wie herkömmliches Geld können diese Währungen verwendet werden, um reale Güter und Dienstleistungen zu kaufen. Digitale Währungen wie Bitcoin sind bekannt als „dezentrale digitale Währungen“, d. h. es gibt keine zentrale Steuerungsstelle für die Geldmenge. (siehe Wikipedia)

[0004] Bitcoin ist Kryptographie-basiertes elektronisches Geld (CBEM), das 2008 erfunden wurde. Bitcoin ist nicht nur virtuelles Geld, sondern auch ein Zahlungssystem, das aus einem dezentralen Peer-to-Peer-Transaktionsnetzwerk zur Aufzeichnung und Verifizierung der Geldtransaktionen besteht.

[0005] Jedem Bitcoin-Besitzer wurde eine oder mehrere eindeutige Bitcoin-Adressen zugewiesen und er besitzt eine Software, die als Kunden-Wallet bezeichnet wird. Bitcoins (d. h. Einheiten der Kryptowährung) werden nicht in den Kunden-Wallets einzelner Besitzer gespeichert, sondern ihr Besitz wird in einem Public Ledger aller Bitcoin-Transaktionen, d. h. der Blockchain, unter Verwendung von Bitcoin-Adressen der Besitzer verzeichnet. Eine Bitcoin-Adresse ist ein 160-Bit-Hash des öffentlichen Teils eines öffentlich/privaten Elliptic Curve Digital Siganture Alorithm-(ECDSA) -Schlüsselpaars. Der private Schlüssel für jede Bitcoin-Adresse wird in dem Kunden-Wallet des Adressbesitzers gespeichert.

[0006] Darüber hinaus sind alle Kunden-Wallets über das Internet miteinander verbunden und bilden Knoten eines Transaktionsnetzwerks, um die Transaktionen weiterzuleiten und zu verifizieren. Unter Verwendung von Public/Private-Key-Kryptografie kann man „signieren“ (d. h. seinen/ihren privaten Schlüssel verwenden), um eine Menge Bitcoins, die an seiner/ihrer Bitcoin-Adresse aufgezeichnet sind, an eine andere Bitcoin-Adresse zu senden. In der Regel kann, wenn die Transaktion von einem privaten Schlüssel signiert wurde, jeder im Transaktionsnetzwerk überprüfen, ob die Signatur gültig ist. Darüber hinaus kann jeder im Transaktionsnetzwerk den Public Ledger überprüfen, um zu bestimmen, ob die Transaktion gültig ist, d. h. ob die Partei, die Bitcoins überträgt, tatsächlich so viele Bitcoins zum Übertragen besaß.

[0007] Seit 2008 wurden verschiedene Kryptographie-basierte elektronische Währungen erschaffen und werden kollektiv als alternative Kryptowährungen bezeichnet. Unter ihnen verwenden einige dieser anderen Bitcoins andere kryptographische Hash-Algorithmen (z. B. Litecoin) und/oder weisen zusätzliche Funktionen auf (z. B. CinniCoin), während einige zur Verwendung anderer Signaturtechnologien erfunden wurden (z. B. CryptoNote).

[0008] Bitcoin ist absichtlich pseudonym, während alle alternativen Kryptowährungen entweder pseudonym oder anonym sind. Anonyme Kryptowährungen können leicht für Geldwäscheaktivitäten verwendet werden, da alle Sender und Empfänger von Geldtransaktionen nicht ermittelbar sind. Für pseudonyme Kryptowährungen zeigte eine akademische Studie (Meiklejohn S. et al., University of California, San Diego, 2013), dass Hinweise auf Interaktionen zwischen Institutionen identifiziert werden können, indem die Struktur der Beteiligung von Bitcoin-Adressen beim empirischen Einkauf von Waren und Dienstleistungen analysiert wird.

[0009] Mit diesem Ansatz können möglicherweise illegale Aktivitäten auf der Ebene der Institution identifiziert werden, es ist jedoch immer noch nicht möglich, sie auf die Ebene einer einzelnen Person einzuengen. Eine neuere akademische Studie (Koshy P. et al., Pennsylvania State University, 2014) hat gezeigt, dass es möglich ist, eine Bitcoin-Adresse einer IP-Adresse zuzuordnen. Dieser Ansatz ist jedoch nur für weniger als 10% der Bitcoin-Adressen anwendbar. Daher wird allgemein angenommen, dass Bitcoin und andere alternative Kryptowährungen für illegale Aktivitäten wie Geldwäsche verwendet werden können (Bryans D., Indiana Law Journal, 89 (1): 441, 2014).

[0010] Diese pseudonyme/anonyme Eigenschaft macht Bitcoin und alternative Kryptowährungen zu attraktiven Zielen für Hacker und Diebe. Zum Beispiel meldete im Februar 2014 die Firma Mt. Gox, die zu dieser Zeit die weltweit größte Bitcoin-Börse war, Konkurs an, da das Unternehmen ständig gehackt

wurde, was zu einem Verlust von 850.000 Bitcoins (im Wert von etwa 480 Millionen US-Dollar) führte.

[0011] Im Januar 2015 wurde die slowenische Bitcoin-Börse Bitstamp, die zu dieser Zeit die drittgrößte Bitcoin-Börse der Welt war, gehackt, und weniger als 19.000 BTC (im Wert von etwa 5 Millionen US-Dollar) wurden gestohlen. Obwohl die Hacker/Diebe die gestohlenen Bitcoins an ihre Bitcoin-Adressen übertragen müssen, bleiben die Identitäten der meisten dieser Hacker und Diebe unbekannt.

[0012] Daher werden Diebstahlschutz-Lösungen für Bitcoin benötigt. Der Besitz von Bitcoins wird durch private Schlüssel geschützt, die in dem Wallet des Nutzers gespeichert sind. Private Schlüssel können aus einer Passphrase erstellt werden. Brainwallet ist beispielsweise eine Website, die ein Werkzeug zum Erzeugen einer Bitcoin-Adresse und ihres privaten Schlüssels aus dem sha256 einer Passphrase bereitstellt. Unter Verwendung eines Passwort-Wörterbuchs könnte man die Bitcoin-Blockchain analysieren und nach aktiven Bitcoin-Adressen suchen, die aus typischen Passwörtern erzeugt wurden, und die Bitcoins von diesen Adressen stehlen, indem die entsprechenden privaten Schlüsseln abgeleitet und verwendet werden.

[0013] Eine einfache Diebstahlschutz-Lösung besteht darin, die Verwendung von Bitcoin-Adressen zu vermeiden, die aus typischen Passphrasen erzeugt wurden. Bei anderen Bitcoin-Adressen können Hacker die Computer oder Server von Bitcoin-Besitzern hacken, um nach Dateien zu suchen, die die Datensätze der privaten Schlüssel enthalten. Sobald diese Dateien entdeckt wurden, können Bitcoins, die an den zugehörigen Adressen gespeichert sind, leicht auf eine andere Adresse übertragen werden. Die einfachste Lösung hierfür ist, solche Dateien in einem kalten Speicher (d. h. einem Gerät, das nicht mit dem Internet verbunden ist) zu speichern oder sogar solche Dateien gar nicht zu erzeugen.

[0014] Eine weitere Möglichkeit, Bitcoins zu stehlen, besteht darin, die Hauptdatei des Wallets (d. h. die Datei „wallet.dat“) in einem Bitcoin-Wallet zu stehlen, das auf einem Computer oder Server installiert ist, der mit dem Internet verbunden ist. Robert Lipovsky (2013) berichtete von einem Online-Banking-Trojaner, der die wallet.dat-Dateien stehlen kann. Private Schlüssel sind in den wallet.dat-Dateien gespeichert und sind mit Passphrasen geschützt. Sobald die Hauptdatei des Wallets gestohlen wurde, kann die Schutz-Passphrase durch Wörterbuch-Raten, Permutationen von Wörterbuch-Wörtern oder reine Brute-Force geknackt werden.

[0015] Ein Beispiel für Lösungen für solche gestohlenen Bitcoin-Wallets ist in der Patentanmeldungsveröffentlichung CN103927656 (A) mit dem Titel „Bitcoin Terminal Wallet with Embedded, Fixed Collecting Address and Bitcoin Payment Method of Bitcoin Terminal Wallet“ beschrieben.

[0016] Eine einfache Lösung für das Obige besteht darin, Bitcoins an einer Mehrfachsignaturadresse zu speichern, einer Währungsadresse, die zwei private Schlüssel zum Ausgeben der Bitcoins benötigt. Ein privater Schlüssel wird in einem Computergerät (z. B. einem lokalen Computer) gespeichert, während ein anderer Schlüssel in einem separaten Computergerät (z. B. einem Smartphone, einem entfernten Server) gespeichert wird, wodurch eine Zwei-Faktor-Authentifizierung für Transaktionen erzeugt wird. Eine solche Lösung ist bis zur vorliegenden Erfindung noch nicht verfügbar.

[0017] Eine weitere Lösung besteht darin, alle Bitcoin-Sender und -Empfänger identifizierbar zu machen. Die rechtlichen Identitäten der Diebe oder Hacker können dann aufgedeckt werden, indem die rechtlichen Identitäten der Besitzer der Bitcoin-Adressen, die die gestohlenen Bitcoins erhalten, öffentlich gemacht werden. Eine solche Lösung ist bis zur vorliegenden Erfindung noch nicht verfügbar.

[0018] Gegenwärtig sind Anti-Geldwäsche- (AML) -Lösungen für Bitcoin sehr gefragt. Damit Bitcoin-Dienstleister die US-amerikanischen (FinCEN) und weltweiten Vorschriften für AML einhalten, besteht der gegenwärtige Ansatz in einer kombinierten Nutzung von Know-Your-Customer (KYC) und Transaktionsüberwachung. Um dies zu ermöglichen, müssen alle Händler/Kunden ihre rechtlichen Identitäten angeben und einer Verifizierung unterzogen werden. Dieser Ansatz leidet jedoch unter zwei Hauptproblemen. Erstens wird dieser Ansatz hauptsächlich von Unternehmen übernommen, die legale Dienstleistungen anbieten. Daher können AML-Aktivitäten mit Bitcoins immer noch weltweit stattfinden. Zweitens haben Unternehmen in der Regel ihre eigenen Systeme zur Kundenregistrierung und Identitätsverifizierung.

[0019] Dies führt nicht nur zu Ressourcenredundanz und hohen Betriebskosten, sondern erzeugt auch Ärger für Bitcoin-Nutzer. Als ehrlicher Bitcoin-Nutzer muss man möglicherweise verschiedenen Bitcoin-Dienstleistern Identitätsdokumente zur Identitätsverifizierung vorlegen, bevor man ihre Dienste nutzen kann.

[0020] Am 25. Februar 2015 startete die Bank of England ihre One Bank Research Agenda - einen ehrgeizigen und umfassenden Rahmen, um die Art und Weise, wie Forschung in der Bank betrieben wird, zu verändern. Laut diesem Diskussionspapier untersucht die Bank of England, ob die Zentralbanken selbst die Blockchain-Technologie von Bitcoin nutzen sollten, um ihre eigenen digitalen Währungen auszugeben. Die Bank of England hat erklärt, dass Pro-

bleme im Zusammenhang mit KYC und AML angegangen werden müssen und untersucht werden sollte, wie digitale Identitätsverwaltung erreicht werden kann, während die Privatsphäre berücksichtigt wird.

[0021] Unter Berücksichtigung des Vorstehenden wäre es vorteilhaft, ein Verfahren zur persönlichen Identifizierung und Verifizierung, ein pseudonymes System und ein Transaktionsnetzwerk zum Überwachen und Beschränken von Transaktionen von Kryptographie-basiertem elektronischem Geld zu entwickeln, die zumindest einige der oben genannten Nachteile vermeiden würden.

[0022] Die vorliegende Erfindung - ein „mit rechtlicher Identität verknüpftes Anmeldeinformations-Authentifizierungsprotokoll“ - ist das erste Protokoll, das eine praktische Lösung für die Probleme im Zusammenhang mit Kryptowährungsdiebstahl, KYC und AML bietet, während die Privatsphäre der Nutzer gewahrt bleibt.

[0023] Nicht zuletzt kann die vorliegende Erfindung von den Zentralbanken oder anderen Finanzinstitutionen angenommen oder modifiziert werden, um ihre eigenen digitalen Währungen auszugeben, die durch ein Distributed Ledger-Zahlungssystem unterstützt werden, aber auch von einem zentralen Leitungsorgan reguliert werden. Der Public Ledger kann privat oder für die Öffentlichkeit zugänglich sein. Solche digitalen Währungen können daher die Vorteile des bestehenden Bankensystems und die Vorteile von Kryptographie-basiertem elektronischem Geld übernehmen.

ZUSAMMENFASSUNG

[0024] Ausführungsformen der Erfindung, die hierin präsentiert werden, können durch die folgenden Abschnitte zusammengefasst werden.

1. Verfahren zur persönlichen Identifizierung und Verifizierung von Transaktionen, die Kryptographie-basiertes elektronisches Geld beinhalten, wobei das Verfahren von einem Rechenserver (101) ausgeführt wird, der zumindest ein Computerprogramms umfasst, das als Registrierungsschnittstelle (102) dient, und das Verfahren dadurch gekennzeichnet ist, dass es die Schritte umfasst von:

• Gewähren des Zugangs für einen oder mehrere potentielle oder bestehende Währungsnutzer (103);

• Bereitstellen einer Registrierungsschnittstelle (102) für einen oder mehrere potenzielle Währungsnutzer zum Registrieren eines Nutzerkontos, das eine Authentifizierung erfordert (104);

• Aufforderung zum Übermitteln von Unterlagen zum Nachweis der rechtlichen Identität eines Registranten (105);

• Verifizieren der rechtlichen Identität des Registranten (106);

• Ablehnen einer Kontoerstellung für Registranten, deren Verifizierung der rechtlichen Identität scheitert (107);

• Erstellen eines Personen/Kundenkontos (108) für einzelne erfolgreiche Registranten (109) mit erfolgreicher Verifizierung der rechtlichen Identität (110);

• Ermöglichen, dass ein erfolgreicher Registrant (109) Anmeldeinformationen (111) erstellt, die eine zugehörige Authentifizierung (112) umfassen;

• Speichern (116) aller übermittelten Informationen in einer Kunden-Informationsdatenbank (115);

• Senden (117) der Anmeldeinformationen an zentrale Genehmigungsserver (401); und

• Zuordnen und Speichern (118) einer oder mehrerer Mehrfachsignatur-Währungsadressen, der Anmeldeinformationen und der rechtlichen Identität einzelner Registranten.

Das Obige kann ferner eines oder mehrere der folgenden umfassen:

(i) die Authentifizierung kann mittels eines Passwortschutzes, einer Zwei-Faktor-Authentifizierung oder einer Mehr-Faktor-Authentifizierung erfolgen;

(ii) einen Schritt zum Verschlüsseln der Anmeldeinformationen (114); und/oder

(iii) der Berechtigungsnachweis ist ein digitales, elektronisches oder Hardwareobjekt, das als ein Authentifizierungsmechanismus verwendet werden kann, um sich zu identifizieren. Zum Beispiel kann es ein eindeutiges Paar digitaler Codes sein (z. B. Name und Passwort); es kann ein eindeutiger Produktschlüssel zur Aktivierung einer Kunden-Wallet-Software sein; und es kann ein sich ständig änderndes Token (z. B. ein eindeutiger 7-stelliger Code) sein, das an ein physisches Gerät gebunden ist, das dem Nutzer gehört, wie beispielsweise ein Mobiltelefon oder ein personalisiertes Gerät zum Erzeugen eines sicheren Schlüssels.

2. Verfahren zum Erzeugen eines Kryptographie-basierten elektronischen Geldes (CBEM) (201) und seines zugehörigen Transaktionsnetzwerks (202), wobei das Verfahren durch ein Netzwerk von Computerprogrammen ausgeführt wird, die als Knoten (203) dienen, und das

Verfahren dadurch gekennzeichnet, dass es die Schritte umfasst von:

• Installieren eines Knotens (203), der ein eigenständiges Computerprogramm oder ein Funktionsmodul eines Kunden-Wallet (111) sein kann, in einem oder mehreren Kundencomputern und/oder -Servern (204);

• Verbinden aller Knoten über ein Datenübertragungsnetzwerk (206), um Relaisknoten (205) eines Peer-to-Peer-Netzwerks zu bilden;

• Steuern des Verfahrens zum Erzeugen mindestens einer Einheit des CBEM (207); Schützen des Besitzes von mindestens einer Einheit des CBEM durch Public/Private-Key-Kryptographie (208);

• Aufzeichnen des Besitzes von mindestens einer Einheit des CBEM in einen Public Ledger aller Transaktionen (z. B. die Blockchain) (209) unter Verwendung der Währungsadressen der Besitzer (313) (210);

• Verifizieren des Besitzes von mindestens einer Einheit des CBEM (211);

• Beschränken der Erzeugung einer oder mehrerer gültiger Währungsadressen (313) nur auf gültig registrierte Nutzer (109), um mindestens eine Einheit des CBEM zu empfangen, indem die übermittelten Anmeldeinformationen (111) mit einem der zentralen Genehmigungsserver verifiziert werden (401) (212);

• Aufzeichnen von Transaktionen von mindestens einer Einheit des CBEM in den Ledger (209) (213);

• Verifizieren von Transaktionen von mindestens einer Einheit des CBEM (214);

• Steuern des Verfahrens zum Übertragen mindestens einer Einheit des CBEM (215); Integrieren der Transaktionsregeln in den Programmcode von mindestens einem Knoten (216);

• Beschränken mindestens einer Transaktionsgenehmigungsregel (217), umfassend mindestens eines von: Anfordern von gültigen Anmeldeinformationen (111) vom Sender, Anfordern eines oder mehrerer privater Genehmigungsschlüssel (406) von einem der zentralen Genehmigungsserver (401);

• Gestatten der Erzeugung nur von Mehrfachsignaturtransaktionen im Pay-to-Script-Hash-Format oder einem anderen kompatiblen Format (218);

• Gestatten der Erzeugung nur von Mehrfachsignaturtransaktionen, von denen jede mindestens zwei private Schlüssel als Signaturen benötigt (219);

• Gestatten der Erzeugung nur von Mehrfachsignaturtransaktionen in Anwesenheit von gültigen Anmeldeinformationen (111) (220);

• Beschränken eines dieser privaten Schlüssel (219) auf einen privaten Genehmigungsschlüssel (406) von einem der zentralen Genehmigungsserver (221);

• Beschränken des Rests der privaten Schlüssel (219) auf private Kunden-Schlüssel (222), die verschlüsselt sind und in dem einen oder den mehreren Kunden-Wallets (301) gespeichert sind (223);

• Senden aller Transaktionsanfragen von den Kunden-Wallets (301) an einen der zentralen Genehmigungsserver (401), um den privaten Genehmigungsschlüssel zum Signieren der Transaktionen zu erhalten (224); und

• Ablehnen aller Transaktionen, denen irgendeiner der erforderlichen privaten Schlüssel (219) fehlt; (225).

3. Verfahren zur persönlichen Identifizierung und Verifizierung von Transaktionen, die Kryptographie-basiertes elektronisches Geld beinhalten, wobei das Verfahren von einem Computerprogramm ausgeführt wird, das als Kunden-Gerät eines Nutzers fungiert, und das Verfahren dadurch gekennzeichnet ist, dass es die Schritte umfasst von:

• Installieren eines Computerprogramms eines Kunden-Geräts in mindestens einem Computer oder Rechenserver (302), um als Kunden-Wallet zu dienen (301);

• Arbeiten als einer der Relaisknoten (205) zum Weiterleiten von Informationen aller CBEM-Einheiten (z. B. Münzen), die in dem Transaktionsnetzwerk (202) erzeugt werden (303); Arbeiten als einer der Relaisknoten (205) zum Weiterleiten aller Transaktionsinformationen in dem Transaktionsnetzwerk (202) (304);

• Arbeiten als einer der Relaisknoten zum Verifizieren und Bestätigen aller Transaktionen, die an das Transaktionsnetzwerk (202) gesendet werden (305);

• Erzeugen neuer Münzen durch Beitrag zur Aufzeichnung neuer Transaktionsinformationen in den Ledger aller Transaktionen (z. B. die Blockchain) (209) (306);

• Erzeugen eines oder mehrerer Paare aus kryptographischem öffentlichem Kunden-Schlüssel (307) und privatem Kunden-Schlüssel (308) zum Empfangen und Senden von Münzen (309);

• Speichern der öffentlich-privaten Kunden-Schlüsselpaare (Elemente 307, 308) einer oder

mehrerer von den Währungsnutzern (310) erzeugten Währungsadressen;

• Arbeiten als Kunden-Wallet für die Währungsnutzer, um Münzen zu empfangen und zu senden; (311);

• Arbeiten als Kunden-Wallet zum Kommunizieren zwischen einem der zentralen Genehmigungsserver (401) und registrierten Währungsnutzern (109) (312);

• Erzeugen (314) nur von Währungsadressen, die Mehrfachsignaturadressen sind (313);

• Erzeugen einer von mehreren Mehrfachsignaturadressen (313) aus dem öffentlichen Kunden-Schlüssel (307) und dem öffentlichen Genehmigungsschlüssel (405) (315);

• Speichern nur von einer oder mehreren Mehrfachsignaturadressen (313) in dem Kunden-Wallet (301) zum Senden und Empfangen von Münzen (316);

• Senden einer von mehreren Mehrfachsignaturadressen (313) an die Kunden-Informationsdatenbank (401) zum Speichern und Zuordnen zu der rechtlichen Identität des Besitzers der einen oder mehreren Adressen (317);

• Senden der erzeugten gültigen Mehrfachsignaturadressen (313) an die zentralen Genehmigungsserver (401) zum Speichern (318);

• Übermitteln von Anmeldeinformationen (111) eines gültig registrierten Nutzers (109) an einen der zentralen Genehmigungsserver zum Erhalten einer Genehmigung zum Erzeugen einer oder mehrerer gültiger Mehrfachsignaturadressen (313) (319);

• Übermitteln von Anmeldeinformationen (111) eines gültig registrierten Nutzers (109) an einen der zentralen Genehmigungsserver zum Erhalten einer Genehmigung zum Erzeugen einer oder mehrerer gültiger Transaktionen (Elemente 218, 219, 220, 221, 223), um Münzen an einen oder mehrere Währungsadressen zu senden (320);

• Gestatten der Erzeugung nur von Transaktionen, die Mehrfachsignaturadressen (313) sowohl zum Senden als auch zum Empfangen der Münzen verwenden (321); und

• Aufzeichnen von nicht ausgegebenen Münzen (falls vorhanden) in die Blockchain an der Währungsadresse, von der die Münzen gerade gesendet wurden (322).

4. Verfahren zur persönlichen Identifizierung und Verifizierung für Transaktionen, die Kryptographie-basiertes elektronisches Geld beinhalten, wobei das Verfahren von einem Computerprogramm in einem als zentralem Genehmigungsserver (401) dienenden Rechenserver ausgeführt wird und das Verfahren dadurch gekennzeichnet ist, dass es die Schritte umfasst von:

• Kommunizieren (407) mit einem Kunden-Wallet (301), um eine oder mehrere gültige Mehrfachsignatur-Währungsadressen (313) in Anwesenheit von gültigen Anmeldeinformationen zu erzeugen;

• Bereitstellen (408) eines öffentlichen Genehmigungsschlüssels (405) für das Währungs-Wallet, um eine oder mehrere Mehrfachsignaturadressen zu erzeugen (313),

• Kommunizieren (409) mit dem Kunden-Wallet (301), um eine oder mehrere gültige Transaktionen (218, 219, 220, 221, 223) zu erzeugen, um Münzen in Anwesenheit von gültigen Anmeldeinformationen an eine oder mehrere Währungsadressen zu senden;

• Bereitstellen (410) eines privaten Genehmigungsschlüssels (406), der zu dem öffentlichen Genehmigungsschlüssel (405) gehört, der bei der Erzeugung der Mehrfachsignaturadresse (313) verwendet wurde, um eine Transaktionseingabe für eine oder mehrere gültige Transaktionen zu signieren (218, 219, 220, 221, 223);

• Bereitstellen des jüngsten privaten Schlüssels (411) zum Signieren der gesamten Transaktion für eine oder mehrere gültige Transaktionen (412); und

• Speichern von Transaktionsinformationen (414) in einer Transaktionsdatenbank (413);

Verfahren nach einem oder allen der obigen Abschnitte, gekennzeichnet durch eine oder mehrere der folgenden Weisen:

dass der letzte private Genehmigungsschlüssel (411) der private Genehmigungsschlüssel, der zu dem öffentlichen Genehmigungsschlüssel (405) gehört, der bei der Erzeugung der Mehrfachsignaturadresse (313) verwendet wurde, oder ein anderer privater Genehmigungsschlüssel ist;

dass der Schritt des Speicherns (414) von Transaktionsinformationen in einer Transaktionsdatenbank (413) das Speichern einer Transaktions-ID, der Sender-Währungsadresse, der Empfänger-Währungsadresse, der Menge der übertragenen Münzen, der Transaktionszeit und der IP-Adresse der Kunden-Wallets des Senders und des Empfängers umfasst;

dass das Verfahren ferner einen Schritt des Verifizierens der Transaktion gegen ein oder mehrere Transaktionskriterien (501, 502) auf dem zentralen Genehmigungsserver (401) aufweist;

dass das eine oder die mehreren Transaktionskriterien (501, 502) Kriterien umfassen, die durch ein zentrales Leitungsorgan (601) und/oder den Registranten vorgegeben sind; und/oder

dass das Verfahren ferner einen Schritt des Ermittelns von rechtlichen Identitäten des Senders und des Empfängers durch Zuordnen ihrer Währungsadressen in der Transaktionsdatenbank und der Kunden-Informationsdatenbank bei Bedarf aufweist.

5. Verfahren zur persönlichen Identifizierung und Verifizierung für Transaktionen, die Kryptographie-basiertes elektronisches Geld beinhalten, wobei das Verfahren durch eine Gruppe von Computerprogrammen, die als Einrichtungen eines zentralen Leitungsorgans dienen, und ein Kunden-Gerät eines Nutzers ausgeführt wird, wobei das Verfahren dadurch gekennzeichnet ist, dass es die Schritte umfasst von:

• Empfangen von Anmeldeinformationen eines Registranten, umfassend mindestens Anmeldeinformationen mit Zwei-Faktor-Authentifizierung, die eine Mehrfachsignatur definieren;

• Verifizieren der rechtlichen Identität des Registranten;

• Erstellen eines Personen/Kundenkontos (108) für einen einzelnen erfolgreichen Registranten (109) mit erfolgreicher Verifizierung der rechtlichen Identität (110), während das Personen/Kundenkonto die Zuordnung und Speicherung der Mehrfachsignatur einer Währungsadresse und der rechtlichen Identität einzelner Registranten erlaubt (118);

• Bereitstellen eines Registranten-Wallet, das mindestens eine Einheit von elektronischem Geld umfasst;

• Aufzeichnen des Besitzes der mindestens einen Einheit von elektronischem Geld in eine Transaktionsdatenbank (413) unter Verwendung der Währungsadresse des Registranten (313);

• Erzeugen einer Mehrfachsignaturtransaktion in einem Pay-to-Script-Hash-Format oder einem anderen kompatiblen Format (218), die jeweils mindestens zwei private Schlüssel als Genehmigungssignaturen benötigt (219);

• Beschränken eines dieser privaten Schlüssel (219) auf einen privaten Genehmigungsschlüssel (406) von einem der zentralen Genehmigungsserver (221);

• Beschränken des Rests der privaten Schlüssel (219) auf die privaten Schlüssel des Registranten (222), die in dem Kunden-Wallet (301, 223) gespeichert sind;

• Senden der Transaktionsanfrage von dem Kunden-Wallet (301) an mindestens einen der zentralen Genehmigungsserver (401), um den privaten Genehmigungsschlüssel zum Signieren der Transaktion zu erhalten (224); und

• Senden der genehmigten Transaktionsnachrichten an alle Relaisknoten in einem Transaktionsnetzwerk (214).

6. System zur persönlichen Identifizierung und Verifizierung von Transaktionen, die Kryptographie-basiertes elektronisches Geld beinhalten, wobei das System umfasst:

• einen zentralen Genehmigungsserver (401), der konfiguriert ist, um das Verfahren gemäß Abschnitt 7 auszuführen, um Kunden-Registrierungsanfragen, Kunden-Kryptowährungsadressen und Kryptowährungstransaktionen zu verarbeiten;

• eine Kunden-Informationsdatenbank (404), die kommunikativ mit dem zentralen Genehmigungsserver (401) verbunden ist;

• eine Transaktionsdatenbank (413), die kommunikativ mit dem zentralen Genehmigungsserver (401) verbunden ist;

• mindestens ein Kunden-Gerät (414, 415), das mit einem Registranten-Wallet (416, 417) versehen ist, das mindestens eine Einheit von elektronischem Geld umfasst;

• wobei das mindestens eine Kunden-Gerät (414, 415) konfiguriert ist, um das Verfahren gemäß einem oder mehreren der obigen Abschnitte auszuführen.

7. Computerprogramm mit Programmcodemitteln zum Ausführen aller Schritte des computerimplementierten Verfahrens gemäß einem oder mehreren der obigen Abschnitte, wenn das Programm auf einem Computer oder einem Rechenserver ausgeführt wird.

8. Computerlesbares Medium, das computerausführbare Befehle speichert, die alle Schritte des computerimplementierten Verfahrens gemäß einem oder mehreren der obigen Abschnitte ausführen, wenn sie auf einem Computer oder einem Rechenserver ausgeführt werden.

9. Verfahren nach einem oder mehreren der vorhergehenden Abschnitte, wobei das Paar aus öffentlichem Genehmigungsschlüssel (405) und privatem Genehmigungsschlüssel (406) in einem regelmäßigen Zeitraum manuell oder automatisch geändert werden kann, um ein Lecken des öffentlichen Genehmigungsschlüssels und des privaten Genehmigungsschlüssels an die Öffentlichkeit zu vermeiden. Nach dem Wechsel zu einem neuen Paar von Genehmigungsschlüsseln wird der alte private Genehmigungs-

schlüssel zum Signieren der Transaktionseingabe (410) verwendet und der neue private Genehmigungsschlüssel wird zum Signieren der gesamten Transaktion (d. h. aller Transaktionsdaten) (412) verwendet.

10. Verfahren nach einem oder mehreren der obigen Abschnitte, wobei jegliche Währungsadressen, die nicht durch die Übermittlung von gültigen Anmeldeinformationen an einen der zentralen Genehmigungsserver (401) erzeugt wurden, nicht gültig sind und keine Münzen erhalten können.

[0025] Verfahren nach einem oder mehreren der obigen Abschnitte, wobei das Transaktionsnetzwerk (202) modifiziert werden kann, um jegliche Transaktionen abzulehnen, die nicht die zentralen Transaktionskriterien (501) oder die Kunden-Transaktionskriterien (502) erfüllen, die in einem der zentralen Genehmigungsserver (401) gespeichert sind.

[0026] Verfahren nach einem oder mehreren der obigen Abschnitte, wobei eines oder mehrere der folgenden hinzugefügt werden können:

die Kunden-Transaktionskriterien können durch einen gültig registrierten Nutzer definiert werden, um seine/ihre eigenen Transaktionen zu begrenzen;

die Transaktionskriterien (501) können von einem zentralen Leitungsorgan (601) definiert werden, um verdächtige Transaktionen zu stoppen, die wahrscheinlich in illegale Aktivitäten wie Geldwäsche verwickelt sind;

einzelne Transaktionen können mit einer definierten Regel überwacht werden, um verdächtige Transaktionen zu identifizieren, aufzuzeichnen und zu melden, die wahrscheinlich an illegalen Aktivitäten wie Geldwäsche beteiligt sind;

[0027] Die rechtlichen Identitäten der Besitzer der einzelnen Währungsadressen sind in der Kunden-Informationsdatenbank gespeichert. Bei denjenigen Transaktionen, bei denen der Verdacht auf illegale Aktivitäten besteht, werden die Identitäten der zugehörigen Sender und Empfänger aus der Kunden-Informationsdatenbank extrahiert, indem sie mit den Währungsadressen der Sender und Empfänger ermittelt werden. Anschließend werden die verdächtigen Aktivitäten und die damit verbundenen Kunden-Informationen den Regierungsbehörden unter Berücksichtigung der Vorschriften und Gesetze in den betroffenen Ländern gemeldet;

[0028] Die rechtlichen Identitäten der Besitzer für einzelne Währungsadressen sind in der Kunden-Informationsdatenbank gespeichert. Dies erfüllt die behördliche Anforderung von „Know-Your-Customer“. Dadurch kann das System als Zahlungssystem für kommerzielle Aktivitäten verwendet werden;

[0029] Die rechtlichen Identitäten der Besitzer für einzelne Währungsadressen sind in der Kunden-Informationsdatenbank gespeichert. Diese Informationen sind jedoch für die Öffentlichkeit nicht zugänglich, um die pseudonyme Eigenschaft des Kryptographie-basierten elektronischen Geldes (201) und seines Transaktionsnetzwerks (202) zu erhalten;

[0030] Ein Nutzer kann seine/ihre Anmeldeinformationen (111) ändern, um zu verhindern, dass Münzen aus einer gestohlenen Hauptdatei (z. B. der wallet.dat-Datei) seines/ihres Währungs-Wallets (301) übertragen werden;

(i) rechtliche Identitäten von Besitzern werden für einzelne Währungsadressen in der Kunden-Informationsdatenbank gespeichert, (ii) jegliche Währungsadressen, die nicht durch die Übermittlung von gültigen Anmeldeinformationen an einen der zentralen Genehmigungsserver (401) erzeugt wurden, sind nicht gültig und können keine Münzen empfangen (Abschnitt 18), und (iii) nur gültig registrierte Nutzer haben gültige Anmeldeinformationen (112). Wenn Münzen von jemandem gestohlen werden, können der oder die Diebstähle oder Hacker leicht ermittelt werden, indem die eine oder mehreren rechtlichen Identitäten der Empfänger aus der Kunden-Informationsdatenbank gemäß der einen oder den mehreren Währungsadressen des einen oder der mehreren Empfänger abgerufen werden. Daher verhindert die Implementierung des oder der obigen Verfahren, dass eine Kryptowährung gestohlen wird;

(ii) die Menge an Münzen, die ein gültig registrierter Nutzer besitzt, ist vollständig und leicht durch das zentrale Leitungsorgan durch Analysieren der Transaktionsdatensätze in der Transaktionsdatenbank ermittel- und verfolgbar. Neben der Fähigkeit, einzelne Währungsadressen ihren Besitzern zuzuordnen, wird diese einzigartige Eigenschaft durch die Aufzeichnung nicht ausgegebener Münzen (falls vorhanden) an der Währungsadresse, von der die Münzen gerade gesendet/ausgegeben wurden, erweitert (322). Diese einzigartige Eigenschaft ermöglicht Anwendungen des Systems für Finanz- und Bankaktivitäten, insbesondere solche, die von Dritten geprüft werden müssen;

(iii) stellt eine praktische Lösung für die Probleme im Zusammenhang mit Kryptowährungsdiebstahl, KYC und AML unter Wahrung der Privatsphäre der Nutzer bereit; und/oder

(iv) kann von den Zentralbanken oder anderen Finanzinstituten übernommen oder modifiziert werden, um ihre eigenen digitalen Währun-

gen auszugeben, die durch ein Distributed Ledger-Zahlungssystem unterstützt werden, aber auch von einem zentralen Leitungsorgan reguliert werden.

[0031] Ferner ist ein Verfahren offenbart, das ein System zum Erzeugen eines neuen Kryptographie-basierten elektronischen Geldes oder einer Kryptowährung mit ermittelbaren rechtlichen Identitäten von Sendern und Empfängern in allen Geldtransaktionen umfasst. Das Verfahren kann in einem System ausgeführt werden, das Folgendes umfasst:

1. Mindestens einen Server und mindestens eine webbasierte Registrierungsschnittstelle, wobei der mindestens eine Server mindestens einige oder alle der folgenden Funktionen ausführt:

• Gewähren des Zugangs für einen oder mehrere potenzielle oder bestehende Währungsnutzer;

• Bereitstellen einer Online-Schnittstelle für einen oder mehrere potenzielle Währungsnutzer zur Registrierung eines Nutzerkontos mit Passwortschutz, Zwei-Faktor-Authentifizierung oder Mehr-Faktor-Authentifizierung;

• Anfordern der Übermittelung von Dokumenten zum Nachweis der rechtlichen Identität eines Registranten;

• Handhaben der Verifizierung der rechtlichen Identität des Registranten;

• Ablehnen einer Kontoerstellung für Registranten, deren Verifizierung der rechtlichen Identität gescheitert ist;

• Erstellen eines Personen/Kundenkontos für einzelne erfolgreiche Registranten mit erfolgreicher Verifizierung der rechtlichen Identität;

• Ermöglichen eines erfolgreichen Registranten, Anmeldeinformationen zu erstellen, die eine Kennung und ein Passwort umfassen;

• Ermöglichen eines erfolgreichen Registranten, die Anmeldeinformationen und Kontaktinformationen zu ändern;

• Verschlüsseln der Anmeldeinformationen;

• Speichern aller übermittelten Informationen, insbesondere der rechtlichen Identität und der verschlüsselten Anmeldeinformationen, in einer Kunden-Informationsdatenbank;

• Senden der verschlüsselten Anmeldeinformationen, die neu erzeugt oder geändert wurden, an zentrale Genehmigungsserver;

• Zuordnen und Speichern von Währungsadressen, der Anmeldeinformationen und der rechtlichen Identität einzelner Registranten.

[0032] Kryptographie-basiertes elektronisches Geld und sein zugehöriges Transaktionsnetzwerk, wobei es mindestens einige oder alle der folgenden Grundfunktionen und einzigartigen Funktionen ausführt:

1. Grundfunktionen, die denen aller anderen Kryptographie-basierten elektronischen Gelder gleichen

• Bereitstellen von Kunden-Wallet-Software für die Öffentlichkeit;

• Verbinden von Computern oder Servern über die Kunden-Wallets;

• Verwenden der verbundenen Computer oder Server zum Bilden von Relaisknoten eines Transaktionsnetzwerks;

• Erzeugen einer vorgegebenen Menge an Geldeinheiten (Münzen) mit einer vorgegebenen Geschwindigkeit;

• Schützen des Besitzes der Münzen durch Public/Private-Key-Kryptographie;

• Aufzeichnen des Besitzes der Münzen in einen Public Ledger aller Transaktionen (z. B. die Blockchain) unter Verwendung der Währungsadressen der Besitzer;

• Verteilen des Public Ledger aller Transaktionen (z. B. der Blockchain) und seiner Aktualisierungen an Personen, die über das Kunden-Wallet mit dem Transaktionsnetzwerk verbunden sind;

• Ermöglichen, dass ein Besitzer eines privaten Schlüssels eine Menge an Münzen nur sendet, ohne dass eine an der entsprechenden Währungsadresse aufgezeichnete Menge an Münzen überschritten wird, nachdem die erforderliche Transaktionsgebühr abgezogen wurde;

• Senden aller neuen Transaktionsnachrichten an alle Relaisknoten im Transaktionsnetzwerk;

• Verifizieren aller neuen Transaktionsnachrichten an einzelnen Relaisknoten;

• Aufzeichnen der Transaktionsinformationen (einschließlich, aber nicht beschränkt auf Sender-Währungsadresse, Empfänger-Währungsadresse, Menge der übertragenen Münzen, Transaktionsgebühr, Transaktionszeit) in den Public Ledger aller Transaktionen (z. B. die Blockchain);

2. Einzigartige Funktionen

• Beschränken des Erzeugens einer oder mehrerer gültiger Währungsadressen zum Erhalten der Münzen nur auf gültig registrierte Nutzer, indem die übermittelten Anmeldeinformationen mit einem der zentralen Genehmigungsserver verifiziert werden;

• Gestatten der Erzeugung nur von Mehrfachsignaturtransaktionen im Pay-to-Script-Hash-Format oder einem anderen kompatiblen Format;

• Gestatten der Erzeugung nur von Mehrfachsignaturtransaktionen, die jeweils mindestens zwei private Schlüssel als Signaturen benötigen;

• Gestatten der Erzeugung nur von Mehrfachsignaturtransaktionen in Anwesenheit von gültigen Anmeldeinformationen;

• Beschränken eines dieser privaten Schlüssel auf einen privaten Genehmigungsschlüssel von einem der zentralen Genehmigungsserver;

• Beschränken des Rests der privaten Schlüssel auf private Kunden-Schlüssel, die verschlüsselt und in dem oder den Kunden-Wallets gespeichert sind;

• Senden aller Transaktionsanfragen von den Kunden-Wallets an einen der zentralen Genehmigungsserver, um den privaten Genehmigungsschlüssel zum Signieren der Transaktionen zu erhalten;

• Ablehnen aller Transaktionen, denen einer der erforderlichen privaten Schlüssel fehlt;

• Beschränken von Transaktionsgenehmigungsregeln (einschließlich, aber nicht beschränkt auf das Anfordern von gültigen Anmeldeinformationen vom Sender, das Anfordern eines oder mehrerer privater Genehmigungsschlüssel von einem der zentralen Genehmigungsserver zum Signieren der Transaktionseingabe und zum Signieren der gesamten Transaktion) für einzelne Transaktionen auf Verwendung eines „Pay-to-Script-Hash"-Skripts oder jedes anderen kompatiblen Skripts, das in die Quelle des elektronischen Geldes als einziges Skript zur Transaktionserstellung eingebaut ist;

[0033] Mindestens ein Computer oder Server zum Ausführen von Kunden-Wallet-Software, wobei das mindestens eine Kunden-Wallet mindestens einige oder alle der folgenden Grundfunktionen und einzigartigen Funktionen ausführt:

1. Grundfunktionen, die denen aller anderen Kryptographie-basierten elektronischen Gelder gleichen

• Arbeiten als einer der Relaisknoten zum Weiterleiten aller Transaktionsinformationen im Transaktionsnetzwerk;

• Arbeiten als einer der Relaisknoten zum Verifizieren und Bestätigen aller Transaktionen, die an das Transaktionsnetzwerk gesendet werden;

• Erzeugen neuer Münzen durch Beitrag zur Aufzeichnung neuer Transaktionsinformationen in den Public Ledger aller Transaktionen (z. B. die Blockchain);

• Erzeugen eines oder mehrerer Paare aus kryptografischem öffentlichem Kunden-Schlüssel und privatem Kunden-Schlüssel zum Empfangen und Senden von Münzen;

• Speichern der öffentlich-privaten Kunden-Schlüsselpaare einer oder mehrerer von den Währungsnutzern erzeugten Währungsadressen;

• Arbeiten als Kunden-Wallet für die Währungsnutzer, um Münzen zu erhalten und zu senden;

2. Einzigartige Funktionen

• Arbeiten als Kunden-Wallet für die Kommunikation zwischen einem der zentralen Genehmigungsserver und registrierten Währungsnutzern;

• Erzeugen nur von Währungsadressen, die Mehrfachsignaturadressen sind;

• Erzeugen einer oder mehrerer Mehrfachsignaturadressen aus dem öffentlichen Kunden-Schlüssel und dem öffentlichen Genehmigungsschlüssel;

• Speichern einer oder mehrerer Mehrfachsignaturadressen nur in dem Kunden-Wallet zum Senden und Empfangen von Münzen;

• Senden einer oder mehrerer Mehrfachsignaturadressen an die Kunden-Informationsdatenbank zum Speichern und Zuordnen zu der rechtlichen Identität des Besitzers der einen oder mehreren Adressen;

• Senden der erzeugten gültigen Mehrfachsignaturadressen an die zentralen Genehmigungsserver zum Speichern;

• Übermitteln von Anmeldeinformationen eines gültig registrierten Nutzers zu einem der zentralen Genehmigungsserver, um eine Genehmigung zum Erzeugen einer oder mehrerer gültiger Mehrfachsignaturadressen zu erhalten;

• Übermitteln von Anmeldeinformationen eines gültig registrierten Nutzers an einen der zentralen Genehmigungsserver zum Erhalten einer Genehmigung zum Erstellen einer oder mehrerer gültiger Transaktionen, um Münzen an eine oder mehrere Währungsadressen zu senden;

• Gestatten der Erzeugung nur von Transaktionen, die Mehrfachsignaturadressen sowohl zum Senden als auch zum Empfangen der Münzen verwenden;

• Aufzeichnen von nicht ausgegebenen Münzen (falls vorhanden) in der Blockchain an der Währungsadresse, von der die Münzen gerade gesendet wurden;

[0034] Mindestens ein zentraler Genehmigungsserver, wobei der mindestens eine zentrale Genehmigungsserver mindestens einige oder alle der folgenden Funktionen ausführt: Der zentrale Server ist in

Antwort auf das Empfangen einer Kunden-Anfrage nach einer Genehmigung für eine Transaktion (311) konfiguriert, um die Transaktion auf Risiken im Zusammenhang mit Geldwäschebekämpfungs- (AML) - Kriterien zu untersuchen und zu mindestens einem von: Verweigern der Genehmigung für die Transaktion; Verzögern des Gewährens einer Genehmigung für die Transaktion für eine Zeitspanne; und Senden einer Warnung von dem zentralen Server über ein Netzwerk an ein elektronisches Gerät, das zu mit mindestens einem einer Regierungsbehörde, eines Risk-Compliance-Beauftragten, dem Kunden und Personal gehört, das mit dem System verbunden sind, das von dem zentralen Server ausgeführt wird.

[0035] Der zentrale Genehmigungsserver kann in einigen Ausführungsformen so konfiguriert sein, dass er einige oder alle der folgenden Aktionen ausführt:

1. Abrufen neuer oder aktualisierter Anmeldeinformationen und der zugehörigen Währungsadressen aus der Kunden-Informationsdatenbank;

2. Speichern und Aktualisieren der Anmeldeinformationen des Nutzers und der zugehörigen Währungsadressen in der zentralen Genehmigungsdatenbank;

3. Erzeugen, Ändern, Verschlüsseln und Speichern eines oder mehrerer Paare aus öffentlichem Genehmigungsschlüssel und privatem Genehmigungsschlüssel.

4. Kommunizieren mit dem Kunden-Wallet, um bei Vorhandensein von gültigen Anmeldeinformationen eine oder mehrere gültige Mehrfachsignatur-Währungsadressen zu erzeugen;

5. Bereitstellen eines öffentlichen Schlüssels für das Währungs-Wallet, um eine oder mehrere Mehrfachsignaturadressen zu erzeugen,

6. Kommunizieren mit dem Kunden-Wallet, um eine oder mehrere gültige Transaktionen zu erstellen, um Münzen in Gegenwart von gültigen Anmeldeinformationen an eine oder mehrere Währungsadressen zu senden;

7. Bereitstellen eines privaten Genehmigungsschlüssels, der zu dem öffentlichen Genehmigungsschlüssel gehört, der bei der Erstellung der Mehrfachsignaturadresse verwendet wurde, um eine Transaktionseingabe für eine oder mehrere gültige Transaktionen zu signieren.

8. Bereitstellen eines weiteren privaten Genehmigungsschlüssels, bei dem es sich um den privaten Genehmigungsschlüssel handeln kann, der in Element 410 verwendet wurde, oder um den letzten privaten Genehmigungsschlüssel, um die gesamte Transaktion für eine oder mehrere gültige Transaktionen zu signieren.

9. Speichern aller Transaktionsinformationen (einschließlich, aber nicht beschränkt auf Transaktions-ID, Sender-Währungsadresse, Empfänger-Währungsadresse, Menge der übertragenen Münzen, Transaktionsgebühr, Transaktionszeit und IP-Adresse der Kunden-Wallets des Senders und Empfängers) in einer Transaktionsdatenbank.

[0036] Ferner ist ein Verfahren zur persönlichen Identifizierung und Verifizierung für Transaktionen offenbart, die Kryptographie-basiertes elektronisches Geld beinhalten, wobei das Verfahren mindestens einige oder alle der Schritte umfasst von:

1. Verifizieren der rechtlichen Identität eines Registranten;

2. Erstellen eines Personen/Kundenkontos, das durch mindestens Zwei-Faktor-Authentifizierung geschützt ist, für einen einzelnen erfolgreichen Registranten mit erfolgreicher Verifizierung der rechtlichen Identität, während das Personen/Kundenkonto die Zuordnung und Speicherung der rechtlichen Identität und der einen oder mehreren Währungsadressen einzelner Registranten zu dem Personen/Kundenkonto ermöglicht;

3. Empfangen von Anmeldeinformationen eines einzelnen erfolgreichen Registranten, Definieren der Identität des Registranten, des Besitzes einer Währungsadresse und der Senderidentität einer Transaktion;

4. Speichern der rechtlichen Identität und der Anmeldeinformationen des Registranten auf einem oder mehreren zentralen Genehmigungsservern;

5. Bereitstellen eines Registranten-Wallet zum Senden und Empfangen mindestens einer Einheit von elektronischem Geld;

6. Aufzeichnen des Besitzes an mindestens einer Einheit von elektronischem Geld in einen Public Ledger aller Transaktionen (z. B. die Blockchain) unter Verwendung der einen oder mehreren Währungsadressen des Registranten;

7. Empfangen und Verifizieren von Anmeldeinformationen, die von einem Registranten-Wallet bei einer Anfrage zum Erzeugen einer Währungsadresse übermittelt werden, auf einen zentralen Genehmigungsserver;

8. Genehmigen der Erstellung einer Mehrfachsignaturadresse als gültige Währungsadresse, die zu dem Registranten gehört, durch Bereitstellen eines öffentlichen Genehmigungsschlüssels von dem zentralen Genehmigungsserver an das Registranten-Wallet;

9. Erzeugen einer gültigen Währungsadresse zum Empfangen von mindestens einer Einheit von elektronischem Geld durch Kombinieren des

öffentlichen Schlüssels des Registranten und des öffentlichen Genehmigungsschlüssels des zentralen Genehmigungsservers in dem Registranten-Wallet;

10. Speichern und Zuordnen der rechtlichen Identität des Registranten, der Anmeldeinformationen und einer oder mehrerer gültiger Währungsadressen in einer Kunden-Informationsdatenbank;

11. Erstellen einer Transaktion in einem „Pay-to-Script-Hash"-Format oder einem anderen kompatiblen Format, die jeweils mindestens zwei private Schlüssel als Signaturen benötigt, in dem Registranten-Wallet;

12. Beschränken mindestens eines dieser privaten Schlüssel auf einen privaten Genehmigungsschlüssel von einem der zentralen Genehmigungsserver;

13. Beschränken des Rests der privaten Schlüssel auf die privaten Schlüssel der Registranten, die in den Kunden-Wallets gespeichert sind;

14. Beschränken von Transaktionsgenehmigungsregeln (einschließlich, aber nicht beschränkt auf das Anfordern von gültigen Anmeldeinformationen vom Sender und das Anfordern eines oder mehrerer privater Genehmigungsschlüssel von einem der zentralen Genehmigungsserver zum Signieren der Transaktionseingabe und zum Signieren der gesamten Transaktion) für einzelne Transaktionen auf die Verwendung eines „Pay-to-Script-Hash"-Skripts oder jedes anderen kompatiblen Skripts, das in der Quelle des elektronischen Geldes als einziges Skript zur Transaktionserstellung eingebaut ist;

15. Empfangen und Verifizieren von Anmeldeinformationen, die von einem Registranten-Wallet bei einer Anfrage zur Erstellung einer Transaktion übermittelt werden, auf einem zentralen Genehmigungsserver;

16. Verifizieren der Transaktion gegen ein oder mehrere Transaktionskriterien (einschließlich, aber nicht beschränkt auf solche, die von dem zentralen Leitungsorgan und/oder dem Registranten vorgegeben sind) auf dem zentralen Genehmigungsserver;

17. Genehmigen der Ausführung der Transaktion durch Signieren der Transaktion mit einem oder mehreren privaten Schlüsseln in dem oder den Registranten-Wallets und durch Signieren der Transaktion mit einem oder mehreren der privaten Genehmigungsschlüssel auf dem zentralen Genehmigungsserver;

18. Aufzeichnen der Transaktionsnachricht in den Ledger aller Transaktionen (z. B. die Blockchain);

19. Speichern der Transaktionsinformationen (einschließlich, aber nicht beschränkt auf die Transaktions-ID, der Kryptowährungsadressen des Senders und Empfängers, der Menge an übertragenen Münzen, der Transaktionszeit und der IP-Adresse der Kunden-Wallets des Senders und Empfängers) in einer Transaktionsdatenbank;

20. Senden der signierten Transaktionsnachricht an alle Relaisknoten in einem Transaktionsnetzwerk zur Bestätigung;

21. Ermitteln von rechtlichen Identitäten des Senders und des Empfängers bei Bedarf durch Zuordnen ihrer Währungsadressen in der Transaktionsdatenbank und der Kunden-Informationsdatenbank.

[0037] Die hierin beschriebenen Systeme und Verfahren können durch eines oder mehrere der folgenden modifiziert werden:

[0038] Die hierin beschriebenen Systeme und Verfahren können modifiziert werden, um zwei oder mehr private Genehmigungsschlüssel von einem oder mehreren unabhängigen zentralen Leitungsorganen zum Genehmigen der Transaktionen anzufordern. Ein solches modifiziertes elektronisches Geld und das damit verbundene Zahlungsnetzwerk können einen höheren Grad an Regulierung und Governance aufweisen.

[0039] Alternativ können die hierin beschriebenen Systeme und Verfahren modifiziert werden, um Einzel-Signaturadressen, die nur von einem einzigen Nutzer signiert werden, oder Mehrfachsignaturadressen, die von zwei oder mehr Nutzern signiert werden, zum Empfangen und Senden von elektronischem Geld zu verwenden, ohne dass ein privater Genehmigungsschlüssel von dem zentralen Leitungsorgan für die Genehmigung der Transaktionen erforderlich ist.

[0040] Eine andere Option anstelle der Verwendung von Mehrfachsignaturverfahren zum Erhalten einer Genehmigung von einem zentralen Server besteht darin, einige oder alle der gleichen Funktionen des einen oder der mehreren zentralen Server auszuführen, indem irgendwelche oder alle dieser Funktionen in einen „Smart Contract" (dt. „intelligenter Vertrag") gesetzt werden, d. h. eine Sammlung von Computerbefehlen, die bestimmte Eingaben oder Bedingungen erfordern, bevor eine Übertragung des CBEM ermöglicht wird. Somit wird ein im Wesentlichen äquivalenter Computercode zu dem, der von dem einen oder den mehreren zentralen Servern ausgeführt würde, durch Platzieren einer oder mehrerer zentraler Serverfunktionen an irgendeinen Punkt zwischen einer Transaktionsnachricht und einer Aufzeichnung der Transaktion auf der Blockchain oder dem verteilten Public Ledger ausgeführt. Smart Contracts kön-

nen Computerprogramme oder Applikationen sein, die die Bedingungen eines Vertrags erfüllen. Zum Beispiel kann ein Smart Contract vorbestimmte Funktionen umfassen, die mit der Erfüllung, Verschlüsselung und Durchsetzung von Vereinbarungen zwischen Personen oder Entitäten verbunden sind. Ein Smart Contract kann ein Abwicklungssystem für die Erfüllung finanzieller oder sonstiger Verpflichtungen bei Eintritt der genannten Bedingungen sein. Solche Bedingungen können die Übertragung von Daten wie einem CBEM, verifizierten Dokumenten, Finanzinstrumenten, Rechtsinstrumenten oder anderen Daten umfassen.

[0041] Die hier beschriebenen Systeme und Verfahren können modifiziert werden, um eine Einzel-Signaturadresse, die nur von einem zentralen Leitungsorgan signiert wird, oder Mehrfachsignaturadressen, die von zwei oder mehr zentralen Leitungsorganen signiert werden, zum Empfangen und Senden von elektronischem Geld zu verwenden, ohne einen privaten Schlüssel von einem Nutzer zur Genehmigung der Transaktionen zu benötigen. Nutzer haben jedoch möglicherweise weniger Schutz beim Besitz ihres elektronischen Geldes. Die Gültigkeit eines solchen modifizierten elektronischen Geldes und des damit verbundenen Zahlungsnetzes kann vom Vertrauen und der Ehrlichkeit des oder der zentralen Leitungsorgane abhängen.

[0042] Die oben beschriebenen Systeme und Verfahren können mindestens einige oder alle der folgenden bevorzugten Merkmale aufweisen:

dass Transaktionen durch das System und/oder den Nutzer rückgängig gemacht werden können, wenn eine Bedingung oder festgelegte Bedingungen nicht erfüllt sind, z. B. nach einer bestimmten Zeitspanne;

dass es vor dem Aufzeichnen einer Transaktion auf einem Public Ledger eine Haltezeit geben kann, wobei ein solches Halten automatisch sein kann, auf Transaktionsgröße und/oder anderen Faktoren basieren kann und mit höherer Transaktionsmenge oder -mengen und/oder Anwesenheit anderer Faktoren zunehmen kann;

dass das System eine mögliche Transaktion und/oder eine tatsächliche Transaktion, z. B. während der Haltezeit, auf AML und/oder andere finanzielle Compliance oder Risiken untersuchen kann;

dass das System jede Transaktion, die gemäß einem Vergleich oder basierend auf einem oder mehreren vorgegebenen Kriterien als verdächtig betrachtet wird, identifizieren und automatisch halten, stoppen und/oder rückgängig machen kann;

dass das eine oder die mehreren solchen vorgegebenen Kriterien Kriterien umfassen können, die AML, KYC, CTF, BSA, FATF und/oder eine oder mehrere Grundsätze für verdächtige Finanztransaktionen anderer Regierungs-, zwischenstaatlicher und/oder anderer Organisationen betreffen;

dass das obige Halten bis zu einer Systembenachrichtigung von einem oder mehreren der folgenden geschaltet werden kann: dem Nutzer, einer dritten Partei, wie zum Beispiel einem Übertragungs-Drittanbieter, und/oder einer anderen Eingabe;

dass das Halten einer Transaktion und/oder ihr Rückgängigmachen auf einer Risikobewertung (z. B. basierend auf einem Compliance-Algorithmus) basieren kann, der vom System empfangen und/oder bestimmt wird, wenn die Risikobewertung einen vorgegebenen Schwellenwert erreicht oder überschreitet, und eine solche Risikobewertung kann basierend auf einer Reihe von Regeln für verdächtige Finanztransaktionen berechnet werden, die Risiken umfassen können, die mit einem oder mehreren der folgenden Elemente verbunden sind: Mittel, die aus riskanten und/oder illegalen Quellen stammen und/oder zu ihnen fließen, z. B. bestimmt durch Daten von Gegenproben von Identitäten verifizierter Nutzer im System gegen eine oder mehrere Listen, z. B. von bekannten und/oder mutmaßlichen Terroristen, bekannten und/oder mutmaßlichen Geldwäschern, bekannten und/oder mutmaßlichen Finanzkriminellen, Kryptowährungs-Diebstahllisten; Cybercrime-Beteiligungslisten; schwarze Listen für FATF und/oder FATF-Risikokriterien; Flugverbotslisten; Indikatoren für Transaktionswäsche; und/oder andere Compliance-Faktoren;

dass das System alleine oder in Verbindung mit anderer Überwachung hierin den Nutzer und/oder Empfänger und/oder Informationen über den Nutzer und/oder den Empfänger gegen eine Liste von IP-Adressen zum Zeitpunkt der Nutzerregistrierung in dem System, jeder Nutzeraktualisierung des Nutzerprofils in dem System, wie zum Beispiel einer Aktualisierung der IP-Adresse, zum Zeitpunkt der Erzeugung einer gültigen Währungsadresse, zum Zeitpunkt einer vorgeschlagenen Transaktion oder Einleitung einer Transaktion, die den Nutzer betrifft, und/oder periodisch überprüfen kann;

dass das System ein Nutzerkonto, z. B. das Konto eines Transaktionsempfängers, basierend auf irgendeinem der obigen Compliance-Faktoren und/oder anderen Faktoren einfrieren kann;

dass das System jede Transaktion an einen Empfänger und/oder einen Nutzer aus einem Land auf einer Sanktionsliste und/oder Embargoliste stoppen und/oder rückgängig machen kann, z. B. basierend auf dem Standort einer IP-

Adresse und/oder basierend auf dem Standort des Nutzer- oder Empfängerprofils im System;

dass das System als Teil eines der Obigen und/oder anderer Finanzkriminalitäts-Erfassungsschritte auch Nutzer auf verdächtige Aktivitäten überwachen kann, z. B. durch Überwachen des Browserverlaufs eines Nutzers auf verdächtige Webaktivität oder z. B. auf Besuch bekannter und/oder mutmaßlicher Webseiten von Terroristen;

dass das System zusätzlich zur Erfassung und/oder Überwachung verdächtiger Aktivitäten Warnungen als Reaktion auf die Erfassung solcher verdächtigen Aktivitäten ausgeben kann, wobei solche Warnungen auf einer Nutzerschnittstelle wie einem Computerbildschirm angezeigt werden können oder akustische Warnungen und/oder andere Warnungen sein können, vorzugsweise für Personal, das mit dem zentralen Server und/oder System verbunden ist, und optional für jeden Nutzer, vorzugsweise nur für unschuldige (nicht-verdächtige) Nutzer, etwa unschuldige Nutzer, die an einer gemeldeten Transaktion beteiligt sind;

dass das System anstelle der obigen Warnungen und/oder zusätzlich dazu und/oder für jede potentielle Transaktion und/oder potentiellen Empfänger und/oder andere Partei einer möglichen Transaktion eine Risikobewertung des oben erwähnten Typs bereitstellen kann;

dass das System ein Wallet verwenden kann, das über typische Mehrfachsignaturkanäle mit dem System kommuniziert, um eine Signatur für eine Transaktion anzufordern und/oder auf eine Anforderung nach einer Signatur für eine Transaktion für einen Nutzer zu antworten, wobei dieser Nutzer die Transaktion signiert haben kann aber nicht muss;

dass das System eine Anforderung zum Signieren von einem Nutzer empfangen kann und das Halten einer Transaktion durch Zurückhalten des Signierens erreichen kann, bis bestimmte Bedingungen erfüllt sind, und/oder eine Transaktion im Hinblick auf einen Schwellenwert des Risikos und/oder einen Schwellentyp des Risikos, ob die Transaktion Teil von Finanzkriminalität ist, nicht signieren muss;

dass das System dies für jede seiner Aktionen hierin als Reaktion auf eine mögliche Transaktion, wie etwa eine Nutzersignatur der Transaktion, durchführen kann;

dass das System SAR-, STR- und/oder verwandte Bericht-Compliance-Software umfassen kann, z. B. zum Erzeugen von SAR- und/oder STR- und/oder anderen erforderlichen Berichten, ausgelöst durch Systemerkennung einer verdächtigen Transaktion und/oder eines verdächtigen Nutzers; und

dass der Nutzer eine Online- und/oder eine Offline-Wallet mit dem System verwenden kann.

[0043] Vorzugsweise können das Paar von öffentlichem Genehmigungsschlüssel und privatem Genehmigungsschlüssel manuell oder automatisch in einem regelmäßigen Zeitraum geändert werden, um ein Lecken des öffentlichen Genehmigungsschlüssels und des privaten Genehmigungsschlüssels an die Öffentlichkeit zu vermeiden. Nach dem Wechsel zu einem neuen Paar von Genehmigungsschlüsseln wird der alte private Genehmigungsschlüssel zum Signieren der Transaktionseingabe verwendet und der neue private Genehmigungsschlüssel zum Signieren der gesamten Transaktion (d. h. aller Transaktionsdaten) verwendet.

[0044] Vorzugsweise sind alle Währungsadressen, die nicht durch die Übermittlung von gültigen Anmeldeinformationen an einen der zentralen Genehmigungsserver erzeugt werden, ungültig und können keine Münzen erhalten.

[0045] Vorzugsweise kann das Transaktionsnetzwerk modifiziert werden, um jegliche Transaktionen abzulehnen, die nicht die zentralen Transaktionskriterien erfüllen, die auf einem der zentralen Genehmigungsserver gespeichert sind.

[0046] Vorzugsweise können die Kunden-Transaktionskriterien durch einen gültig registrierten Nutzer definiert werden, um seine/ihre eigenen Transaktionen zu begrenzen.

[0047] Vorzugsweise können die Transaktionskriterien von einem zentralen Leitungsorgan definiert werden, um verdächtige Transaktionen zu stoppen, die wahrscheinlich an illegalen Aktivitäten wie Geldwäsche beteiligt sind.

[0048] Vorzugsweise können einzelne Transaktionen mit einer definierten Regel überwacht werden, um verdächtige Transaktionen zu identifizieren, aufzuzeichnen und zu melden, die wahrscheinlich an illegalen Aktivitäten wie Geldwäsche beteiligt sind.

[0049] Vorzugsweise werden rechtliche Identitäten von Besitzern einzelner Währungsadressen in der Kunden-Informationsdatenbank gespeichert. Bei denjenigen Transaktionen, bei denen der Verdacht auf illegale Aktivitäten besteht, werden die Identitäten der zugehörigen Sender und Empfänger aus der Kunden-Informationsdatenbank extrahiert, indem sie mit den Währungsadressen der Sender und Empfänger ermittelt werden. Anschließend werden die verdächtigen Aktivitäten und die damit verbundenen Kunden-Informationen den Regierungsbehörden un-

ter Berücksichtigung der Vorschriften und Gesetze in den betroffenen Ländern gemeldet.

[0050] Vorzugsweise werden die rechtlichen Identitäten von Besitzern für einzelne Währungsadressen in der Kunden-Informationsdatenbank gespeichert. Dies erfüllt die behördliche Anforderung von „Know-Your-Customer“. Dadurch kann das System als Zahlungssystem für kommerzielle Aktivitäten verwendet werden.

[0051] Vorzugsweise werden die rechtlichen Identitäten von Besitzern für einzelne Währungsadressen in der Client-Informationsdatenbank gespeichert. Solche Informationen sind jedoch für die Öffentlichkeit nicht zugänglich, um die pseudonyme Eigenschaft des Kryptographie-basierten elektronischen Geldes und seines Transaktionsnetzwerks zu erhalten.

[0052] Vorzugsweise kann ein Nutzer seine/ihre Anmeldeinformationen ändern, um zu verhindern, dass Münzen aus einer gestohlenen Hauptdatei (z. B. der wallet.dat-Datei) seines/ihres Währungs-Wallets übertragen werden. Vorzugsweise (i) werden rechtliche Identitäten von Besitzern für einzelne Währungsadressen in der Kunden-Informationsdatenbank gespeichert, (ii) sind Währungsadressen, die nicht durch die Übermittlung von gültigen Anmeldeinformationen an einen der zentralen Genehmigungsserver erzeugt wurden, nicht gültig und sind nicht in der Lage, Münzen zu erhalten, und nur gültig registrierte Nutzer haben gültige Anmeldeinformationen. Wenn Münzen von jemandem gestohlen wurden, können der oder die Diebstähle oder Hacker leicht ermittelt werden, indem die eine oder mehreren rechtlichen Identitäten der Empfänger aus der Kunden-Informationsdatenbank abgerufen werden. Daher verhindert die Implementierung des Systems, dass Kryptowährung gestohlen wird.

[0053] Vorzugsweise ist die Menge an Münzen, die ein gültig registrierter Nutzer besitzt, vollständig und leicht durch das zentrale Leitungsorgan durch Analysieren der Transaktionsdatensätze in der Transaktionsdatenbank ermittel- und verfolgbar. Neben der Fähigkeit, einzelne Währungsadressen ihren Besitzern zuzuordnen, wird diese einzigartige Eigenschaft durch die Aufzeichnung von nicht ausgegebenen Münzen (falls vorhanden) an der Währungsadresse, von der die Münzen gerade gesendet/ausgegeben wurden, verbessert. Diese einzigartige Eigenschaft ermöglicht Anwendungen unseres Systems für Finanz- und Bankaktivitäten, insbesondere solche, die von Dritten geprüft werden müssen.

[0054] Vorzugsweise bieten die Systeme eine praktische Lösung für die Probleme im Zusammenhang mit Kryptowährungsdiebstahl, KYC und AML, während die Privatsphäre der Nutzer erhalten bleibt.

[0055] Vorzugsweise können die Systeme von den Zentralbanken oder anderen Finanzinstituten übernommen oder modifiziert werden, um ihre eigenen digitalen Währungen auszugeben, die durch ein Distributed Ledger-Zahlungssystem unterstützt werden, aber auch von einem zentralen Leitungsorgan reguliert werden.

Figurenliste

[0056] Diese und weitere Ziele der hier vorgestellten Erfindung werden durch Bereitstellen eines Systems und Verfahrens zur persönlichen Identifizierung und Verifizierung gelöst. Weitere Einzelheiten und Merkmale der vorliegenden Erfindung, ihre Natur und verschiedene Vorteile werden aus der folgenden detaillierten Beschreibung der in einer Zeichnung gezeigten bevorzugten Ausführungsformen deutlicher werden, in denen:

Fig. 1 ein Registrierungs- und Datenbanksystem zum Erfassen, Verifizieren und Speichern der rechtlichen Identität eines neuen Nutzers für ein Kryptographie-basiertes elektronisches Geld zeigt;

Fig. 2 ein mit rechtlicher Identität verknüpftes Anmeldeinformations-Authentifizierungssystem zur Erzeugung einer Mehrfachsignatur-Währungsadresse zum Empfangen und Senden eines Kryptographie-basierten elektronischen Geldes zeigt;

Fig. 3 ein mit rechtlicher Identität verknüpftes Anmeldeinformations-Authentifizierungssystem und das Zwei-Parteien-Signaturschema zur Erzeugung einer Zahlungstransaktion einer Menge von Münzen zeigt, die einem Nutzer gehören und an einer Mehrfachsignaturadresse verzeichnet sind;

Fig. 4 ein Diagramm eines Systems gemäß der vorliegenden Erfindung zeigt;

Fig. 5 ein beispielhaftes Flussdiagramm für ein Halten und/oder ein Rückgängigmachen einer Transaktion basierend auf Risikofaktoren ist;

Fig. 6 ein Flussdiagramm ist, das Komponenten eines Risikobewertungsmoduls zeigt; und

Fig. 7 ein Systemdiagramm einer Variante einer Ausführungsform oder von Ausführungsformen ist, wobei ein Smart Contract verwendet wird.

BEZUGSZEICHEN UND FACHBEGRIFFE

[0057] Einige Abschnitte der folgenden detaillierten Beschreibung sind in Form von Datenverarbeitungsvorgängen, -schritten oder anderen symbolischen Darstellungen von Operationen an Datenbits gezeigt, die auf einem Computerspeicher ausgeführt werden können. Somit führt ein Computer solche logischen

Schritte aus, was physische Manipulationen physischer Größen erfordert.

[0058] Üblicherweise haben diese Größen die Form von elektrischen oder magnetischen Signalen, die in einem Computersystem gespeichert, übertragen, kombiniert, verglichen und anderweitig manipuliert werden können. Aus Gründen der allgemeinen Verwendung werden diese Signale als Bits, Pakete, Nachrichten, Werte, Elemente, Symbole, Zeichen, Begriffe, Zahlen oder dergleichen bezeichnet.

[0059] Außerdem müssen alle diese und ähnliche Begriffe den geeigneten physischen Größen zugeordnet werden und sind lediglich zweckmäßige Bezeichnungen, die auf diese Größen angewendet werden. Ausdrücke wie „verarbeiten“ oder „erzeugen“ oder „übertragen“ oder „ausführen“ oder „bestimmen“ oder „erfassen“ oder „erhalten“ oder „auswählen“ oder „berechnen“ oder „generieren“ oder dergleichen beziehen sich auf Handlungen und Verfahren eines Computersystems, das Daten, die als physische (elektronische) Größen in den Registern und Speichern des Computers repräsentiert sind, manipuliert und in andere Daten umwandelt, die in ähnlicher Weise als physische Größen in den Speichern oder Registern oder einem anderen derartigen Informationsspeicher repräsentiert sind.

[0060] Ein computerlesbares (Speicher-) Medium, auf das hierin Bezug genommen wird, kann üblicherweise nicht-flüchtig sein und/oder ein nicht-flüchtiges Gerät umfassen. In diesem Zusammenhang kann ein nicht-flüchtiges Speichermedium ein Gerät umfassen, das greifbar sein kann, was bedeutet, dass das Gerät eine konkrete physische Form aufweist, obwohl das Gerät seinen physischen Zustand ändern kann. So bezieht sich beispielsweise „nicht-flüchtig“ auf ein Gerät, das trotz einer Zustandsänderung greifbar bleibt.

[0061] Wie hier verwendet, bedeutet der Ausdruck „Beispiel“, dass er als nicht einschränkendes Beispiel, Variante oder Darstellung dient. Wie hierin verwendet, führen die Begriffe „zum Beispiel“ und „z. B.“ eine Liste von einem oder mehreren nicht einschränkenden Beispielen, Varianten oder Darstellungen ein.

BESCHREIBUNG DER AUSFÜHRUNGSFORMEN

[0062] Die vorliegende Erfindung betrifft technische Gebiete von Kryptographie-basiertem elektronischem Geld (CBEM), wie zum Beispiel alternative Kryptowährungen und Transaktionssysteme. Insbesondere betrifft die vorliegende Erfindung ein Verfahren und System zum Erzeugen eines neuen CBEM und des zugehörigen Zahlungssystems, das die Offenlegung der rechtlichen Identitäten von Sendern und Empfängern in allen Geldtransaktionen ermöglicht, während die pseudonyme Eigenschaft des CBEM erhalten wird.

[0063] Die vorliegende Erfindung ermöglicht die Einbeziehung zusätzlicher Module zur Überwachung aller Transaktionen und zur Identifizierung derjenigen, die möglicherweise mit illegalen Aktivitäten in Verbindung stehen, und zur Aufnahme von Kriterien, die von einem zentralen Leitungsorgan oder von CBEM-Nutzern definiert werden, um Transaktionen zu regulieren oder zu begrenzen.

[0064] Als Ergebnis liefert die vorliegende Erfindung eine praktische Lösung für die Probleme im Zusammenhang mit Kryptowährungsdiebstahl, KYC und AML, während die Privatsphäre der Nutzer gewahrt bleibt. Darüber hinaus kann die vorliegende Erfindung von den Zentralbanken oder anderen Finanzinstitutionen übernommen oder modifiziert werden, um ihre eigenen digitalen Währungen auszugeben, die durch ein Distributed Ledger-Zahlungssystem unterstützt werden, aber auch von einem zentralen Leitungsorgan reguliert werden.

[0065] Zu diesem Zweck umfasst die vorliegende Erfindung eine Integration von drei Hauptverfahren, unter anderem (i) Verifizierung der rechtlichen Identität, (ii) Authentifizierung von Anmeldeinformationen und (iii) ein Zwei-Parteien-Signaturschema. Ausführungsformen der vorliegenden Erfindung können Systeme und Verfahren zum Erzeugen eines CBEM und seines zugehörigen Bezahlsystems vorsehen, die es einem zentralen Leitungsorgan ermöglichen, rechtliche Identitäten von Sendern und Empfängern bei beliebigen Geldtransaktionen offenzulegen, während die pseudonyme Eigenschaft des CBEM erhalten wird.

[0066] Der Anmeldeinformations-Authentifizierungsmechanismus der vorliegenden Erfindung ermöglicht es einem Nutzer, die Anmeldeinformationen zu ändern, um zu verhindern, dass Münzen aus einem gestohlenen Wallet übertragen werden. Und schließlich können, da Sender und Empfänger aller Transaktionen offengelegt werden können, der eine oder die mehreren Diebstähle oder Hacker, die die Münzen gestohlen haben, leicht durch Abrufen der einen oder mehreren rechtlichen Identitäten der Empfänger aus der Kunden-Informationsdatenbank ermittelt werden. Folglich können die Ausführungsformen der vorliegenden Erfindung verhindern, dass CBEM-Münzen gestohlen werden.

[0067] Um die rechtlichen Identitäten von Sendern und Empfängern aller Transaktionen eines CBEM offenlegen zu können, benötigt es die folgenden zwei Schlüsselelemente:

1. die rechtliche Identität aller Empfänger und Sender eines CBEM;

2. das Verbot, dass anonyme Personen Münzen eines CBEM empfangen und senden.

[0068] Diese zwei Schlüsselelemente können erhalten werden, indem nur registrierte Nutzer mit einer verifizierten rechtlichen Identität ein CBEM empfangen und senden können. Für die Erfassung und Verifizierung der rechtlichen Identität wird eine webbasierte Registrierungsschnittstelle erstellt, die es einzelnen Registranten ermöglicht, Informationen zu übermitteln, um seine/ihre rechtliche Identität zu übermitteln und nachzuweisen, und nur Personen mit einer erfolgreich verifizierten rechtlichen Identität werden als gültige Nutzer akzeptiert. Sie können dann das CBEM empfangen und senden. Die Hauptschwierigkeit besteht jedoch darin, zu verhindern, dass anonyme Personen Münzen eines CBEM, insbesondere eines Open-Source-CBEM, empfangen und senden.

[0069] Kryptographie-basiertes elektronisches Geld (CBEM) kann digitale Währung jeder Art sein, die ähnliche Eigenschaften wie physische Währungen aufweist, aber sofortige Transaktionen, kryptografische Sicherheit und digitale oder virtuelle Eigentumsübertragung ermöglicht. Beispiele für CBEM sind virtuelle Währungen, Kryptowährungen, Kryptowertpapiere (z. B. elektronische/digitale Wertpapiere oder mit Wertpapieren verbundene Wertmarken) oder sogar von der Zentralbank ausgegebenes „digitales Zentralbankgeld“. Das CBEM kann auch alle Arten von elektronischen/digitalen Wertmarken (engl. „Token“) (die z. B. ein Zertifikat oder einen Vertrag als Nachweis des Besitzes einer Unternehmensaktie, Nachweis von Kapitalbeteiligung, Nachweis eines Gewinnbeteiligungsrechts für ein Unternehmen oder Nachweis des Lizenzanteilsrechts für ein Patent usw. repräsentieren), alle Arten von elektronischen/digitalen Zertifikaten für PoE (z. B. Berechtigungsnachweis) und jedes andere geeignete digitale oder virtuelle Tauschmedium umfassen. Kryptographie wird häufig in einem CBEM verwendet, um Geräte und Nachrichten zu authentifizieren und Daten vor unbefugter Beobachtung oder Änderung zu schützen. Beispiele für CBEM umfassen Bitcoin, Ether, Ripple, Litecoin, Dash oder andere geeignete Kryptowährungen.

[0070] CBEM-Transaktionen können unabhängig von ihrem Typ in einem verteilten Netzwerk gespeichert werden, beispielsweise verteilten Speichern, einem Distributed Ledger, einer Blockchain oder einem anderen geeigneten Mechanismus für verteilte Transaktionen. Ein verteilter Speicher kann Dateien oder Dateisegmente umfassen, die auf einem oder mehreren Netzwerkknoten gespeichert sind. Der verteilte Speicher ist nicht auf ein bestimmtes Format oder Protokoll beschränkt, sondern kann Dateien eines beliebigen Typs umfassen, die auf jedem zugänglichen Netzwerkknoten gespeichert sind, wie zum Beispiel Servern, Desktops, mobilen Geräten, entfernbaren Speichern oder anderen geeigneten Geräten. In einer Ausführungsform kann eine Datei in ihrer Gesamtheit auf einem einzelnen Knoten gespeichert werden und eine andere Datei in einem anderen Netzwerkknoten gespeichert werden. Alternativ kann eine einzelne Datei in eine Mehrzahl von Segmenten aufgeteilt und auf einem oder mehreren Netzwerkknoten gespeichert werden.

[0071] CBEMs, wie Bitcoin, sind als dezentrales Zahlungssystem konzipiert. Es wird erwartet, dass ihre Computerprogrammcodes für jedermann in der Open-Source-Online-Community zugänglich sind.

[0072] Wenn ein CBEM Open Source ist, kann jeder den Quellcode verwenden, um seine/ihre Währungsadresse zum Empfangen und Senden der Münzen zu erstellen.

[0073] Daher kann der KYC-Registrierungsansatz nur auf bestimmte Diensteanbieter angewendet werden, nicht jedoch auf alle Münzen-Nutzer.

[0074] Ein Distributed Ledger kann aus einer Datenbank oder Kopien einer Datenbank bestehen, die über ein verteiltes Netzwerk oder Netzwerke geteilt und synchronisiert werden. Der Distributed Ledger ermöglicht es, dass Transaktionen öffentlich oder privat angezeigt und repliziert werden können, wodurch ein Cyberangriff erschwert wird. Der Distributed Ledger kann auch einen Konsens über die Existenz und den Status von geteilten Fakten in vertrauenslosen Umgebungen aufrechterhalten (d. h., wenn die Teilnehmer, die die gemeinsam genutzte Datenbank hosten, unabhängige Akteure sind, die einander nicht vertrauen). Konsens ist kein Alleinstellungsmerkmal des Distributed Ledger an sich: Andere verteilte Datenbanken verwenden ebenfalls Konsensalgorithmen, etwa Paxos oder Raft. Gleiches gilt für die Unveränderbarkeit: Unveränderbare Datenbanken existieren außerhalb von DLs (Google HDFS, Zebra, CouchDB, Datomic usw.).

[0075] Der Distributed Ledger kann sich wie folgt von einer allgemeinen verteilten Datenbank unterscheiden: (a) Die Steuerung des Lese-/Schreibzugriffs ist wirklich dezentral und nicht wie bei anderen verteilten Datenbanken logisch zentralisiert, und daher es ist möglich, (b) Transaktionen in konkurrierenden Umgebungen ohne vertrauenswürdige Dritte zu sichern. Distributed Ledger-Strukturen können linear sein, z. B. die Blockchain, oder gerichtete azyklische Diagramme (DAG) umfassen, beispielsweise Iota Tangle. Die Blockchain, Iota Tangle und Hedera Hashgraph sind spezifische Beispiels eines Distributed Ledger mit vorgegebenen Formaten und Zugriffsprotokollen.

[0076] Die Blockchain ist ein Distributed Ledger, der CBEM-Transaktionen chronologisch speichert. In einem Blockchain-Ledger werden alle CBEM-Transaktionen periodisch verifiziert und in einem „Block“ gespeichert, der über einen kryptografischen Hash mit dem vorhergehenden Block verknüpft ist. Der Blockchain-Ledger ist öffentlich einsehbar, sodass die Öffentlichkeit CBEM-Transaktionen einsehen und verfolgen kann. Jeder Netzwerkknoten kann eine Kopie der Blockchain erhalten und verwalten.

[0077] Um die Münznutzung auf nur registrierte Nutzer zu beschränken, wurde ein neues Verfahren entwickelt, um von registrierten, nicht anonymen Nutzern erzeugte Währungsadressen (d. h. gültige Währungsadressen) von denen zu unterscheiden, die von nicht registrierten anonymen Nutzern erzeugt wurden (d. h. ungültige Währungsadressen), und ein weiteres Verfahren wurde entwickelt, um nur diese gültigen Währungsadressen zum Empfangen und Senden von Münzen zu verwenden.

[0078] Die vorliegende Erfindung sieht eine praktische Lösung für diese beiden Aufgaben durch eine Integration von drei Hauptverfahren vor, unter anderem (i) Identitätsüberprüfung, (ii) Authentifizierung von Anmeldeinformationen und (iii) ein Zwei-Parteien-Signaturschema. Eine solche Integration erfordert technische Änderungen bei:

1. Modifizieren des Bitcoin-Mehrfachsignatur-Transaktionsprotokolls;

2. Verknüpfen mit einer Kunden-Informationsdatenbank;

3. Festlegen als obligatorisches Transaktionsprotokoll, und

4. Erzwingen, dass eine Transaktionssignatur ein privater Schlüssel von einem der zentralen Genehmigungsserver ist.

[0079] Die Ausführungsformen der vorliegenden Erfindung können durch die folgenden Hauptschritte erreicht werden:

Schritt 1: Einrichten eines Computerservers und einer webbasierten Schnittstelle zum Erfassen, Verifizieren und Speichern rechtlicher Identitäten von Nutzern und zum Erstellen nutzerspezifischer Anmeldeinformationen;

Schritt 2: Verwenden der webbasierten Nutzerschnittstelle zum Erstellen von Anmeldeinformationen zum Regulieren des Verfahrens der Währungsadressenerzeugung;

Schritt **3**: Verwenden eines Mehrfachsignatur-Ansatzes zum Empfangen und Senden von Münzen; und

Schritt 4: Erzwingen von Pay-to-Script-Hash-Transaktionen, die durch bestimmte Regeln reguliert werden.

[0080] Die zuvor erwähnten Schritte werden nun detaillierter beschrieben.

Schritt 1: Einrichten eines Computerservers und einer webbasierten Schnittstelle zum Erfassen, Verifizieren und Speichern rechtlicher Identitäten von Nutzern und zum Erstellen nutzerspezifischer Anmeldeinformationen

[0081] Der Schritt zum Einrichten eines Computerservers und einer webbasierten Schnittstelle (z. B. BGCwallet.com) betrifft Nutzer eines CBEM (z. B. Aten Coin). Beim Vorgang der Registrierung sollte eine Person Dokumente/Informationen über seine/ihre rechtliche Identität (z. B. Pass-Seriennummer und Kopie der Datenseite seines/ihres Passes) zur Verfügung stellen und ein Verfahren zum Verifizieren seiner/ihrer rechtlichen Identität durchlaufen (z. B. den Identitätsprüfungsdienst von MiiCard oder IDchecker). Eine erfolgreiche Registrierung erfordert ein erfolgreiches Verifizieren seiner/ihrer rechtlichen Identität. Alle bereitgestellten Informationen werden in einer Kunden-Informationsdatenbank gespeichert.

[0082] **Fig. 1** zeigt ein Registrierungs- und Datenbanksystem zum Erfassen, Verifizieren und Speichern der rechtlichen Identität eines neuen Nutzers für ein Kryptographie-basiertes elektronisches Geld.

[0083] Mindestens ein Server, der mindestens eine webbasierte Registrierungsschnittstelle (**102**) umfasst, führt die folgenden Funktionen aus. Zuerst wird in Schritt (**105**) über die webbasierte Registrierungsschnittstelle (**102**) eine Übermittlung von Dokumenten zum Nachweis der rechtlichen Identität eines Registranten angefordert. Als nächstes wird in Schritt (**106**) die Verifizierung der rechtlichen Identität des Registranten durchgeführt. Eine erfolglose Verifizierung führt zu einem Registrierungsfehler (**107**). Alternativ dazu kann ein erfolgreicher Registrant (**109**) eine Zwei-Faktor-Authentifizierung oder eine Multi-Faktor-Authentifizierung (**104**) erstellen, um einen nicht autorisierten Zugriff auf sein/ihr registriertes Nutzerkonto und böswillige Angriffe zu verhindern.

[0084] Die Zwei-Faktor-Authentifizierung ist ein sicheres Verfahren zum Schutz eines Online-Nutzerkontos (**104**). Sie funktioniert so, dass ein Nutzer sich mit zwei verschiedenen Objekten identifizieren muss, wenn er/sie sich in seinem/ihrem Online-Konto anmeldet. Das erste Authentifizierungsobjekt ist ein Paar aus Login-Name und Login-Passwort, die vom Nutzer erstellt werden; das zweite Authentifizierungs-

objekt ist ein sich ständig änderndes Token (z. B. ein eindeutiger 7-stelliger Code), das an ein physisches Gerät gebunden ist, das dem Nutzer gehört, beispielsweise ein Mobiltelefon oder ein personalisiertes Gerät zum Erzeugen eines sicheren Schlüssels. Dann kann ein solches Online-Nutzerkonto nicht gehackt werden, ohne das persönliche physische Gerät zu stehlen. Eine Multi-Faktor-Authentifizierung kann auch möglich sein, bei der ein Nutzer sich bei Anmeldung in seinem/ihrem Online-Konto mit drei oder mehr verschiedenen Objekten identifizieren muss (z. B. einem Paar von Login-Namen und Login-Passwort, einem Mobiltelefon und einem intelligenten Personalausweis).

[0085] Ein erfolgreicher Registrant (**109**) muss Anmeldeinformationen (**111**) erstellen, die eine Kennung und ein Passwort (**112**) umfassen. Natürlich kann ein erfolgreicher Registrant (109) die Anmeldeinformationen und Kontaktinformationen (**113**) ändern, die alle vorzugsweise in Schritt (**114**) verschlüsselt werden. Die Anmeldeinformationen werden benötigt, damit ein Nutzer seine/ihre eine oder mehreren Mehrfachsignatur-Wallet-Adressen (**Fig. 2**) zum Empfangen von Münzen (z. B. Atencoins) und zum Erstellen von Transaktionen (**Fig. 3**) erzeugen kann.

[0086] Optional können bei Schritt **502** Kunden-Transaktionskriterien durch einen gültig registrierten Nutzer definiert werden, um seine/ihre eigenen Transaktionen zu begrenzen. Zum Beispiel kann ein Nutzer ein Kriterium festlegen, das die maximale Menge an Münzen begrenzt, die von seiner/ihrer einen oder mehreren Währungsadressen innerhalb von 24 Stunden gesendet werden können. Dies kann den Verlust seiner/ihrer Münzen minimieren, wenn sein/ihr Währungs-Wallet gestohlen oder gehackt wurde.

[0087] Wenn das Obige abgeschlossen ist, wird in Schritt (**116**) das Speichern aller übermittelten Informationen, insbesondere der rechtlichen Identität und der verschlüsselten Anmeldeinformationen, in der Kunden-Informationsdatenbank (**115**) ausgeführt.

[0088] Schließlich wird in Schritt **117** das Senden der verschlüsselten Anmeldeinformationen, die neu erstellt oder geändert wurden, an zentrale Genehmigungsserver (**401**) ausgeführt. Die zentralen Genehmigungsserver führen das Zuordnen und Speichern der einen oder mehreren Mehrfachsignatur-Währungsadressen, der Anmeldeinformationen und der rechtlichen Identität einzelner Registranten (**118**) aus. Zum Beispiel ist eine Mehrfachsignatur-Währungsadresse eine eindeutige Zeichenfolge aus 34 Zeichen, die aus numerischen Zahlen, kleinen und großen Buchstaben bestehen (z. B. Aj8xFoZUjo3GoNvi95kABpTjO2qQReZo5P); die persönliche Identität besteht aus (i) einem vollständigen, auf dem Personalausweis oder Reisepass des Nutzers aufgedruckten rechtlichen Namen, (ii) der Personalausweis-/Reisepassnummer und (iii) dem Geburtsdatum.

[0089] Schritt **2**: Verwenden der webbasierten Nutzerschnittstelle zum Erstellen von Anmeldeinformationen zum Regulieren des Verfahrens der Währungsadresserzeugung

[0090] Unter Verwendung der webbasierten Schnittstelle kann nur ein gültig registrierter Nutzer (**106**, **109**) Anmeldeinformationen (**111**) erzeugen (**Fig. 1**, **Fig. 112**), die zum Erzeugen seiner/ihrer einen oder mehreren Mehrfachsignaturadressen benötigt werden (wie in **Fig. 2** gezeigt), um Münzen (z. B. Atencoins) zu empfangen und zu senden (wie in **Fig. 3** gezeigt). Die Verwendung von Anmeldeinformationen verhindert, dass nicht registrierte, anonyme Nutzer gültige Mehrfachsignaturadressen erzeugen, um Münzen im System zu empfangen und zu senden. Mit anderen Worten sind alle gültigen Währungsadressen zum Senden oder Empfangen von Münzen eines CBEM tatsächlichen Personen mit bekannten, rechtlichen Identitäten zugeordnet.

[0091] Schritt **3**: Verwenden eines Mehrfachsignatur-Ansatzes zum Empfangen und Senden von Münzen

[0092] Absichtlich sind für die Erstellung gültiger Mehrfachsignaturadressen für das Empfangen und Senden von Münzen ein öffentlicher Genehmigungsschlüssel von einem der zentralen Genehmigungsserver und mindestens ein öffentlicher Kunden-Schlüssel erforderlich (**Fig. 2**). Bevor man das Kunden-Wallet (**301**) verwenden kann, um eine Adresse zum Empfangen von Münzen zu erzeugen, muss er/sie seine/ihre Anmeldeinformationen (**111**) in das Kunden-Wallet eingegeben haben. Im Verfahren der Adresserzeugung übermittelt das Kunden-Wallet zuerst die Anmeldeinformationen an einen der zentralen Genehmigungsserver (**401**) über ein elektronisches/digitales Datenübertragungsnetzwerk (z. B. das Internet) zur Validierung (**407**).

[0093] Nach der Überprüfung, ob die Anmeldeinformationen gültig sind, d. h. nach einem erfolgreichen Abgleich mit gültigen und aktiven Anmeldeinformationen in der Datenbank der zentralen Genehmigungsserver (**319**, **401**, **407**), stellt der zentrale Genehmigungsserver den öffentlichen Genehmigungsschlüssel (**408**) dem Kunden-Wallet durch das elektronische/digitale Datenübertragungsnetz bereit. Wenn die Anmeldeinformationen als ungültig oder inaktiv befunden werden, gibt der zentrale Genehmigungsserver eine Fehlernachricht an das Kunden-Wallet zurück. Nach dem Erhalt des öffentlichen Genehmigungsschlüssels fährt das Kunden-Wallet mit dem Erzeugen einer Mehrfachsignaturadresse fort (**315**).

[0094] Nach dem Erhalt der Fehlernachricht stoppt das Kunden-Wallet das Verfahren der Mehrfachsignaturadresserzeugung. In Anwesenheit des öffentlichen Genehmigungsschlüssels erzeugt (**309**) das Kunden-Wallet ein Paar aus öffentlichem Kunden-Schlüssel (**307**) und privatem Kunden-Schlüssel (**308**) und speichert sie (**310**) in dem Kunden-Wallet und kombiniert anschließend den öffentlichen Genehmigungsschlüssel (**405**) und den öffentlichen Kunden-Schlüssel (**307**), um eine Mehrfachsignaturadresse zu erzeugen (**315**), die somit eng mit dem privaten Genehmigungsschlüssel und dem privaten Kunden-Schlüssel verknüpft ist. Die Mehrfachsignaturadresse wird gespeichert und in dem Kunden-Wallet angezeigt (**316**). Der Nutzer kann die Mehrfachsignaturadresse verwenden, um Münzen eines CBEM (z. B. Atencoins) zu empfangen.

[0095] Die Anwesenheit des öffentlichen Genehmigungsschlüssels in jeder Mehrfachsignaturadresse erzwingt, dass alle Transaktionen sowohl die Genehmigungssignatur (d. h. den privaten Genehmigungsschlüssel (**406**)) von einem der zentralen Genehmigungsserver als auch die Kunden-Signatur (d. h. den privaten Kunden-Schlüssel (**308**)) erhalten müssen, um Validität zu erlangen.

[0096] Unter Verwendung dieses Steuersystems können nur gültig registrierte Nutzer Mehrfachsignaturadressen erzeugen. Diese Adressen können dann verwendet werden, um Transaktionen auszuführen, die von einem der zentralen Genehmigungsserver gegengezeichnet werden müssen.

[0097] Fig. 2 zeigt ein mit rechtlicher Identität verknüpftes Anmeldeinformations-Authentifizierungssystem zur Erzeugung einer Mehrfachsignatur-Währungsadresse zum Empfangen und Senden eines Kryptographie-basierten elektronischen Geldes.

[0098] Das Verfahren beginnt bei Schritt (**301**) mit der Bereitstellung eines Kunden-Wallet, das eine Netzwerkressource ist, auf die vorzugsweise als Software zugegriffen werden kann. Als nächstes werden die eingegebenen Nutzer-Anmeldeinformationen von Schritt (**111**) angewendet, um das Wallet eines Nutzers zu aktivieren. Anschließend versucht ein Nutzer bei Schritt (**314**), eine Währungsadresse zu erzeugen, wobei das System nur Währungsadressen erzeugt, bei denen es sich um Mehrfachsignaturadressen handelt.

[0099] Als nächstes wird in Schritt (**319**) das Übermitteln von Anmeldeinformationen von gültig registrierten Nutzern an einen der zentralen Genehmigungsserver (**401**) ausgeführt, um eine Genehmigung zum Erzeugen einer oder mehrerer gültiger Mehrfachsignaturadressen zu erhalten.

[0100] Bei fehlgeschlagener Genehmigung kann eine entsprechende Fehlermeldung erzeugt werden.

[0101] Andernfalls wird im Fall der Genehmigung in Schritt (**309**) das Erzeugen eines oder mehrerer Paare aus einem kryptographischem öffentlichem Kunden-Schlüssel (**307**) und privatem Kunden-Schlüssel (**308**) zum Empfangen und Senden von Münzen ausgeführt. Dieser öffentliche Kunden-Schlüssel und private Kunden-Schlüssel werden gespeichert und dem Wallet des Kunden zugeordnet (**310**). Im Falle einer Genehmigung wird bei Schritt **408** auch das Bereitstellen eines öffentlichen Genehmigungsschlüssels (**405**), der mathematisch mit einem privaten Genehmigungsschlüssel (**406**) verknüpft ist, von dem zentralen Genehmigungsserver an das Kunden-Wallet ausgeführt.

[0102] Ferner wird bei Schritt (**315**) das Erzeugen einer von mehreren Mehrfachsignaturadressen aus dem oder den öffentlichen Kunden-Schlüsseln (**307**) und dem oder den öffentlichen Genehmigungsschlüsseln (**405**) ausgeführt. Die erzeugte Mehrfachsignatur-Währungsadresse wird gespeichert und dem Wallet des Kunden zugeordnet (**316**).

[0103] Anschließend wird in Schritt (**317**) das Senden der einen oder mehreren Mehrfachsignaturadressen an die Kunden-Informationsdatenbank (**115**) zum Speichern und Zuordnen zu der rechtlichen Identität des Besitzers der einen oder mehreren Adressen (**118**) ausgeführt.

[0104] Schritt **4**: Erzwingen von Pay-to-Script-Hash-Transaktionen, die durch bestimmte Regeln reguliert werden

[0105] Bitcoin-Entwickler haben derzeit zwei verschiedene Verfahren zum Erstellen und Genehmigen von Bitcoin-Transaktionen mit unterschiedlichen scriptSig/scriptPubKey-Paaren erstellt. Die beiden Verfahren sind Pay-to-Pubkey-Hash und Pay-to-Script-Hash.

[0106] Der Pay-to-Pubkey-Hash ist das am häufigsten verwendete Verfahren in täglichen Bitcoin-Transaktionen. In einer Pay-to-Pubkey-Hash-Transaktion ist eine Bitcoin-Adresse ein 160-Bit-Hash des öffentlichen Teils eines öffentlich/privaten Elliptic Curve Digital Signature Algorithm-(ECDSA) -Schlüsselpaars und ein Bitcoin-Sender stellt eine Bitcoin-Adresse in scriptPubKey bereit. Bei einer Pay-to-Pubkey-Hash-Transaktion überträgt ein Sender Bitcoins direkt an einen Besitzer eines öffentlichen Schlüssels.

[0107] Um eine Pay-to-Pubkey-Hash-Transaktion zu initiieren, muss der Sender einen öffentlichen Schlüssel, dessen Bitcoins an der zugehörigen Bitcoin-Adresse gespeichert sind, und die zugehörige Signatur (d. h. einen zugehörigen privaten Schlüs-

sel) sowie eine Bitcoin-Adresse bereitstellen, um die Bitcoins zu empfangen. Die empfangende Bitcoin-Adresse ist direkt mit dem zugehörigen öffentlichen Schlüssel und der Signatur verknüpft. Beim Einlösen von Münzen, die an die Bitcoin-Adresse gesendet wurden, stellt der Empfänger sowohl die Signatur als auch den öffentlichen Schlüssel zur Verfügung. Das Skript verifiziert, ob der bereitgestellte öffentliche Schlüssel auf den Hashwert in scriptPubKey hasht, und überprüft dann auch die Signatur anhand des öffentlichen Schlüssels.

[0108] Adressen, die mit Pay-to-Script-Transaktionen verknüpft sind, sind Hashs von Skripten anstelle von Hashs von öffentlichen Schlüsseln. Um Bitcoins über Pay-to-Script-Hash ausgeben zu können, muss das Verfahren ein Skript bereitstellen, das zu dem Skript-Hash und den Daten passt, wodurch das Skript als wahr bewertet wird. Mit anderen Worten muss man dem fraglichen Skript eine Eingabe (d. h. eine Antwort) bereitstellen, die das Skript akzeptiert, und die Transaktion wird fortgesetzt. Wenn die Eingabe ungültig ist und das Skript sie nicht akzeptiert, führt dies zum Abbruch der Transaktion.

[0109] Mit Pay-to-Script-Hash kann man Bitcoins an eine Adresse senden, die auf verschiedene ungewöhnliche Arten abgesichert ist, ohne etwas über die Details zu wissen, wie die Sicherheit eingerichtet ist. Zum Beispiel könnte der Empfänger die Signaturen mehrerer Personen benötigen, um Bitcoins zu erhalten, die an einer bestimmten Bitcoin-Adresse gespeichert sind, oder ein Passwort könnte erforderlich sein, oder die Anforderungen könnten vollständig individuell sein. Für Bitcoin und alle anderen heutigen Kryptowährungen, die auf Basis der Bitcoin-Technologie entwickelt wurden, ist Pay-to-Script-Hash nicht zwingend erforderlich.

[0110] Der Pay-to-Pubkey-Hash ist das Standardverfahren in Bitcoin-Transaktionen sowie in den Transaktionen für alle anderen heutigen Kryptowährungen auf Basis der Bitcoin-Technologie. Die Pay-to-Script-Hash-Funktion ist in der Kunden-Wallet-Software einer Kryptowährung integriert. Ein Kryptowährungsbesitzer kann die Kunden-Wallet-Software dazu verwenden, Pay-to-Pubkey-Hash oder Pay-to-Script-Hash zum Erstellen von Transaktionen zu verwenden.

[0111] Gemäß der vorliegenden Erfindung sind in dem CBEM-Transaktionsnetzwerk nur Pay-to-Script-Hash-Transaktionen erlaubt. Im Gegensatz zu Bitcoin und allen anderen aktuellen Kryptowährungen, die auf der Bitcoin-Technologie basieren, wird diese Einschränkung in den Quellcodes des CBEM implementiert und nicht nur in dem Quellcode der Kunden-Wallet-Software. Auf diese Weise kann ein CBEM-Entwickler in allen Transaktionen spezifische Regeln durchsetzen und dies ermöglicht die Implementierung eines mit rechtlicher Identität verknüpften Anmeldeinformations-Authentifizierungssystems, um alle Transaktionen zu steuern. Das mit rechtlicher Identität verknüpfte Anmeldeinformations-Authentifizierungssystem beinhaltet die Verwendung von nutzerspezifischen Anmeldeinformationen und Mehrfachsignaturadressen zum Empfangen und Senden des CBEM.

[0112] In dem mit rechtlicher Identität verknüpften Anmeldeinformations-Authentifizierungssystem werden nur Mehrfachsignaturadressen in den Pay-to-Script-Hash-Transaktionen zum Empfangen und Senden des CBEM verwendet. Jede Kunden-Mehrfachsignaturadresse ist mit einem Skript verknüpft, das einen öffentlichen Kunden-Schlüssel (der von dem Kunden-Wallet erzeugt wird) (**307**) und einen öffentlichen Genehmigungsschlüssel (der von einem der zentralen Genehmigungsserver erzeugt wird) (**405**) enthält, um Transaktionen zu erzeugen und zu signieren. Daher erfordert jede Pay-to-Script-Hash-Transaktion mindestens einen privaten Kunden-Schlüssel (**308**) und einen privaten Genehmigungsschlüssel (**406**), um die Transaktion gültig zu machen.

[0113] Das Skript für Pay-to-Script-Hash-Transaktionen ist in den Quellcodes des CBEM implementiert und nicht nur in den Kunden-Wallets. Dadurch kann das Skript die Anforderung eines oder mehrerer privater Genehmigungsschlüssel (**406**) von einem oder mehreren zentralen Genehmigungsservern zum Initialisieren und Signieren aller Transaktionen erzwingen. Da die Bereitstellung der privaten Genehmigungsschlüssel über die zentralen Genehmigungsserver reguliert werden kann, kann niemand eine Pay-to-Pubkey-Hash- oder Pay-to-Script-Hash-Transaktion erstellen, die die Anforderungen, Vorschriften und/oder Regeln umgehen kann, die auf den zentralen Genehmigungsservern vorgegeben sind.

[0114] Fig. 3 zeigt ein mit rechtlicher Identität verknüpftes Anmeldeinformations-Authentifizierungssystem und das Zwei-Parteien-Signaturschema zur Erzeugung einer Zahlungstransaktion einer Menge von Münzen, die einem Nutzer gehören und an einer Mehrfachsignaturadresse verzeichnet sind.

[0115] Um eine Pay-to-Script-Hash-Transaktion (**218**) zu erzeugen, benötigt ein Wallet (**301**) eines Nutzers eine Signatur (d. h. einen privaten Genehmigungsschlüssel) (**406**) von einem der zentralen Genehmigungsserver (**401**), um eine Genehmigung zu erhalten. Diese Anfrage wird mit einem API-Aufruf zur Authentifizierung an die zentralen Genehmigungsserver gesendet (**220**). Bei einem Scheitern der Authentifizierung kann eine entsprechende Fehlermeldung erzeugt werden.

[0116] Wenn die von dem Kunden-Wallet an die zentralen Genehmigungsserver (**401**) übermittelten Anmeldeinformationen gültig sind (**220**, **409**) und diese angeforderte Transaktion gemäß vorgegebenen Kriterien (**501**, **502**) nicht als verdächtig betrachtet wird, erhält sie die Signatur von dem Kunden-Wallet (d. h. den privaten Kunden-Schlüssel) (**308**) und die Signaturen von einem der zentralen Genehmigungsserver (d. h. den einen oder die mehreren privaten Genehmigungsschlüssel) (**406**, **411**), um die Transaktion zu genehmigen (**410**, **412**).

[0117] Das Skript eines Pay-to-Script-Hashs kann so geändert werden, dass mehr als ein öffentlicher Kunden-Schlüssel und/oder privater Genehmigungsschlüssel erforderlich sind, was zu Zahlungstransaktionen führt, die mehr als eine Signatur von einem oder mehreren Nutzern (entweder Sendern oder Empfängern) und/oder einer oder mehreren Genehmigungsorganen benötigen, um mit einer Transaktion fortzufahren. Um die Sicherheit zu erhöhen, können ferner zwei verschiedene private Genehmigungsschlüssel zum Signieren der Transaktionseingabe (**410**) und zum Signieren der gesamten Transaktion (**412**) verwendet werden.

[0118] Die vorliegende Erfindung erzwingt, dass alle Transaktionen mindestens einen privaten Genehmigungsschlüssel von einem zentralen Genehmigungsserver als Signatur erfordern, um mit einer Transaktion fortzufahren. Darüber hinaus erfordert das Bereitstellen von privaten Genehmigungsschlüsseln eine erfolgreiche Validierung von gültigen, vom Sender bereitgestellten Anmeldeinformationen. Da alle gültigen Anmeldeinformationen mit individuellen Kunden-Wallet-Adressen verknüpft sind und registrierten Nutzern gehören, von denen rechtliche Identitäten verifiziert und in der Kunden-Informationsdatenbank gespeichert wurden (**Fig. 2**), kann nur ein registrierter Nutzer, dessen rechtliche Identität in der Datenbank gespeichert ist, jegliche Münzen von seinen/ihren Wallet-Adressen an andere Wallet-Adressen übertragen, wenn er/sie gültige Anmeldeinformationen übermittelt hat.

[0119] Die Anmeldeinformationen stellt eine Verbindung für ein zentrales Leitungsorgan bereit, das die zentralen Genehmigungsserver und die Kunden-Informationsdatenbank besitzt, um bei Bedarf die rechtliche Identität eines CBEM-Senders oder -Empfängers aufzudecken. Da im gesamten Verfahren einer Pay-to-Script-Hash-Transaktion keine Informationen über rechtliche Identität benötigt werden, bleiben Sender und Empfänger pseudonym.

[0120] Ein zentraler Genehmigungsserver kann alle Transaktionen ablehnen, die nicht die zentralen Transaktionskriterien erfüllen (**501**), die auf mindestens einem der zentralen Genehmigungsserver (**401**) gespeichert sind. Insbesondere können einzelne Transaktionen mit vorgegebenen Regeln überwacht werden, um verdächtige Transaktionen zu identifizieren, aufzuzeichnen und zu melden, die wahrscheinlich an illegalen Aktivitäten wie Geldwäsche beteiligt sind. Verdächtige Transaktionen und Identitäten der zugehörigen Sender und Empfänger können den zuständigen Regierungsbehörden zur weiteren Bearbeitung gemeldet werden. Die Erfindung stellt somit eine praktische Lösung für die aktuellen KYC/AML-Compliance-Probleme für Bitcoin und verschiedene alternative Währungen bereit.

[0121] Optional können bei Schritt **502** Kunden-Transaktionskriterien durch einen gültig registrierten Nutzer definiert werden, um seine/ihre eigenen Transaktionen zu begrenzen. Zum Beispiel kann ein Nutzer ein Kriterium festlegen, das die maximale Menge an Münzen begrenzt, die von seiner/ihrer einen oder mehreren Währungsadressen innerhalb von 24 Stunden gesendet werden können. Dies kann den Verlust seiner/ihrer Münzen minimieren, wenn sein/ihr Währungs-Wallet gestohlen oder gehackt wurde.

[0122] Die Transaktion wird dann an das Netzwerk von Knoten (**214**) zur Bestätigung gesendet (305). Nachdem eine Transaktion erstellt wurde, wird sie zur Verarbeitung an ihr Transaktionsnetzwerk gesendet und muss in einen Block der Blockchain eingefügt werden, bevor sie legitim wird. Knoten akzeptieren den Block nur, wenn alle darin enthaltenen Transaktionen gültig (d. h. korrekt signiert) sind und das CEBM nicht bereits ausgegeben wurde. Knoten drücken ihre Akzeptanz des Blocks aus, indem sie daran arbeiten, den nächsten Block in der Kette zu erzeugen, wobei der Hash des akzeptierten Blocks als vorheriger Hash verwendet wird.

[0123] Der Vorgang der Implementierung einer Transaktion in einen neu erstellten Block wird Transaktionsbestätigung genannt. Die Aufnahme in einen Block gilt als Bestätigung.

[0124] Wenn es ebenso viele oder mehr Bestätigungen als eine vorgegebene Anzahl gibt (z. B. 6 bei Bitcoin, 10 bei Aten Coin), gilt die Transaktion als bestätigt. Bei der Bitcoin-Technologie wurde diese Funktion eingeführt, um das System vor wiederholtem Ausgeben (d. h. mehrfachem Ausgeben) derselben Münzen zu schützen.

[0125] Die einzigartigen Funktionen der in **Fig. 1-3** gezeigten Anordnung sind:

- Gestatten der Erzeugung nur von Mehrfachsignaturadressen (**313**) als gültige Währungsadressen; (**314**)
- Gestatten der Erzeugung nur von Transaktionen, die Mehrfachsignaturadressen (**313**) so-

wohl zum Senden als auch zum Empfangen der Münzen verwenden; (**321**)

• Gestatten der Erzeugung nur von Transaktionen im Pay-to-Script-Hash-Format oder einem anderen kompatiblen Format (**218**); (**311**) Gestatten der Erzeugung nur von Transaktionen, von denen jede mindestens zwei private Schlüssel als Signaturen benötigt; (**308**, **406**)

• Beschränken eines dieser privaten Schlüssel (**308**, **406**) auf einen privaten Genehmigungsschlüssel (**406**) von einem der zentralen Genehmigungsserver (**401**);

• Beschränken des Rests der privaten Schlüssel (**308**, **406**) auf private Kunden-Schlüssel (308), die verschlüsselt und in dem oder den Kunden-Wallets (**301**) gespeichert sind;

• Beschränken des Erzeugens von gültigen Anmeldeinformationen (**111**) nur auf gültig registrierte Nutzer (**109**); (**112**)

• Beschränken der Erzeugung einer oder mehrerer gültiger Mehrfachsignatur-Währungsadressen zum Empfangen der Münzen (**313**) nur auf Nutzer mit gültigen Anmeldeinformationen (**109**), indem die übermittelten Anmeldeinformationen (**111**) über einen der zentralen Genehmigungsserver verifiziert werden (**401**) (**212**);

• Beschränken der Erzeugung einer oder mehrerer gültiger Transaktionen nur auf Nutzer, die gültige Anmeldeinformationen (**111**), eine oder mehrere gültige Mehrfachsignatur-Währungsadressen (**313**) und die zugehörigen privaten Kunden-Schlüssel (**308**, **309**) haben; (**220**, **320**, **409**)

• Beschränken des Empfangens eines oder mehrerer privater Genehmigungsschlüssel (406, 411) von einem der zentralen Genehmigungsserver (**401**) zum Signieren einer oder mehrerer Transaktionen (**410**, **412**) von auf Nutzer mit gültigen Anmeldeinformationen (**111**) durch Verifizieren (**220**, **320**, **409**) der übermittelten Anmeldeinformationen (**111**) über einen der zentralen Genehmigungsserver (**401**);

• Beschränken des Erstellens gültiger Transaktionen nur auf Nutzer, die einen oder mehrere private Genehmigungsschlüssel (**406**, **411**) von einem der zentralen Genehmigungsserver (**401**) erhalten haben, durch Verifizieren (**220**, **320**, **409**) der übermittelten Anmeldeinformationen (**111**) durch einen der zentralen Zustimmungsserver (**401**) und somit Beschränken des Erzeugens von gültigen Transaktionen nur auf Nutzer, die gültige Anmeldeinformationen (**111**) haben;

• Verknüpfen einzelner Anmeldeinformationen (**111**, **112**, **113**, **114**) mit den rechtlichen Identitäten der Nutzer (**105**); (**Fig. 1**)

• Verwendung individueller Anmeldeinformationen (**Fig. 1**, **Fig. 111**), um die rechtlichen Identitäten ihrer Besitzer zu ermitteln (**105**); (**116**)

• Verknüpfen einzelner Mehrfachsignaturadressen (**313**, **314**) mit den Anmeldeinformationen der Nutzer (**111**); (**Fig. 2**)

• Verwenden einzelner Mehrfachsignaturadressen (**313**) zum Ermitteln (**118**) von Anmeldeinformationen (**111**) ihrer Besitzer (**Fig. 2**) und folglich Verwenden der Anmeldeinformationen (**111**) zum Ermitteln (**116**) von rechtlichen Identitäten (**105**) der Besitzer (**Fig. 1**);

• Verwenden einzelner Transaktionen zum Ermitteln von Mehrfachsignaturadressen (**313**) von Sendern und Empfängern (**Fig. 3**), anschließendes Verwenden der Mehrfachsignaturadressen (**313**) zum Ermitteln (**118**) von Anmeldeinformationen (**111**) der Sender und Empfänger (**Fig. 2**) und schließlich Ermitteln (**116**) rechtlicher Identitäten (105) der Sender und Empfänger unter Verwendung der Anmeldeinformationen (**Fig. 1**, **Fig. 111**);

• Gestatten der Ermittlung und Verfolgung (**116**) von rechtlichen Identitäten von Sendern (**Fig. 1**, **Fig. 105**) und Empfängern in allen gültigen Transaktionen (**Fig. 3**), weil nur Nutzer mit gültigen Anmeldeinformationen (**111**) gültige Mehrsignaturadressen erzeugen können (**Fig. 2**) und gültige Transaktionen erstellen können (**Fig. 3**).

[0126] In einigen Implementierungen können die in Verbindung mit den **Fig. 1**, **Fig. 2** und/oder 3 beschriebenen Verfahren in einer oder mehreren Verarbeitungsvorrichtungen (z. B. einem digitalen Prozessor, einem analogen Prozessor, einer digitalen Schaltung zur Informationsverarbeitung, einer analogen Schaltung zur Informationsverarbeitung, einer Zustandsmaschine und/und oder anderen Mechanismen zur elektronischen Verarbeitung von Informationen) verwendet werden.

[0127] Die eine oder die mehreren Verarbeitungsvorrichtungen können eine oder mehrere Vorrichtungen umfassen, die einige oder alle der Vorgänge des Verfahrens als Reaktion auf Befehle ausführen, die elektronisch auf einem elektronischen Speichermedium gespeichert sind. Die eine oder die mehreren Verarbeitungsvorrichtungen können eine oder mehrere Vorrichtungen umfassen, die durch Hardware, Firmware und/oder Software so konfiguriert sind, dass sie speziell für die Ausführung eines oder mehrerer der Vorgänge des oder der in den **Fig. 1**, **Fig. 2** und/oder 3 gezeigten Verfahren entworfen sind.

[0128] **Fig. 4** zeigt ein Diagramm des Systems gemäß der vorliegenden Erfindung. Das System ist eine Client-Server-Anordnung, bei der der Server aus einem oder mehreren zentralen Genehmigungsservern

besteht. Das Diagramm zeigt ein beispielhaftes Computernetzwerk („System 400“), in dem eine oder mehrere Implementierungen der vorliegenden Erfindung realisiert werden können. In einigen Implementierungen kann das System **400** einen oder mehrere Server 401 umfassen. Der oder die Server **401** können dazu konfiguriert sein, mit einer oder mehreren Client-Computerplattformen **414**/**415** gemäß einer Client/Server-Architektur zu kommunizieren. Die Nutzer können über die eine oder mehreren Client-Computerplattformen **414**/**415** auf das System **400** zugreifen. Der oder die Server **401** und die eine oder mehreren Client-Computerplattformen 414/415 können dazu konfiguriert sein, maschinenlesbare Befehle auszuführen.

[0129] In einigen Implementierungen können der oder die Server **401**, die eine oder mehreren Client-Computerplattformen 414/415 und/oder eine oder mehrere externe Ressourcen **418** operativ über eine oder mehrere elektronische Kommunikationsverbindungen verbunden sein. Zum Beispiel können solche elektronischen Kommunikationsverbindungen zumindest teilweise über ein Netzwerk wie das Internet und/oder andere Netzwerke hergestellt werden. Es versteht sich, dass dies nicht einschränkend sein soll und dass der Umfang dieser Offenbarung Implementierungen umfasst, in denen der oder die Server **401**, die eine oder mehreren Client-Computerplattformen **414**/**415** und/oder die eine oder mehreren externen Ressourcen **418** operativ über andere Kommunikationsmedien verbunden sein können.

[0130] Eine gegebene Client-Computerplattform **414**/**415** kann einen oder mehrere Prozessoren umfassen, die konfiguriert sind, um maschinenlesbare Befehle auszuführen. Die maschinenlesbaren Befehle können konfiguriert sein, um es einem mit der gegebenen Client-Computerplattform 414/415 verbundenem Experten oder Nutzer zu ermöglichen, mit dem System **400** und/oder der einen oder den mehreren externen Ressourcen **418** zu interagieren und/oder andere Funktionalität bereitzustellen, die hier der einen oder den mehreren Client-Computerplattformen zugeschrieben 414/415 werden. Als nicht einschränkendes Beispiel kann die gegebene Client-Computerplattform **414**/**415** einen oder mehrere eines Desktop-Computers, eines Laptop-Computers, eines Handheld-Computers, einer Tablet-Computerplattform, eines Netbooks, eines Smartphones, einer Spielekonsole und/oder andere Computerplattformen umfassen.

[0131] Die eine oder mehreren externen Ressourcen **418** können Informationsquellen, externe Einheiten, die Teil des Systems **400** sind, und/oder andere Ressourcen umfassen. In einigen Implementierungen können einige oder alle der Funktionen, die der einen oder den mehreren externen Ressourcen **418** hier zugeschrieben werden, durch Ressourcen bereitgestellt werden, die in dem System **400** enthalten sind.

[0132] Der oder die Server **401** und/oder die eine oder mehreren Client-Computerplattformen **414**/**415** können elektronischen Speicher **419**, einen oder mehrere Prozessoren **420** und/oder andere Komponenten umfassen. Der oder die Server **401** können Kommunikationsleitungen oder Ports umfassen, um den Austausch von Informationen mit einem Netzwerk und/oder anderen Computerplattformen zu ermöglichen. Die Abbildung des einen oder der mehreren Server **401** in **Fig. 1** soll nicht einschränkend sein. Der oder die Server **401** können eine Mehrzahl von Hardware-, Software- und/oder Firmware-Komponenten umfassen, die zusammenarbeiten, um die Funktionalität bereitzustellen, die hier dem einen oder den mehreren Servern **401** zugeschrieben wird. Zum Beispiel kann der oder die Server **401** durch eine Cloud von Computerplattformen implementiert sein, die zusammen als der oder die Server **401** arbeiten.

[0133] Der elektronische Speicher **419** kann nichtflüchtige Speichermedien umfassen, die Informationen elektronisch speichern. Das elektronische Speichermedium des elektronischen Speichers 419 kann einen Systemspeicher umfassen, der integral (d. h. im Wesentlichen nicht entfernbar) mit dem Server **401** bereitgestellt ist, und/oder entfernbaren Speicher, der mit dem oder den Servern **405**, beispielsweise über einen Port (z. B. einen USB-Port, einen Firewire-Port usw.) oder ein Laufwerk (z. B. ein Diskettenlaufwerk usw.) entfernbar verbunden sein kann. Der elektronische Speicher **419** kann ein oder mehrere optisch lesbare Speichermedien (z. B. optische Platten usw.), magnetisch lesbare Speichermedien (z. B. Magnetband, ein magnetisches Festplattenlaufwerk, ein Diskettenlaufwerk usw.), auf elektrischer Ladung basierende Speichermedien wie Festspeichermedien (z. B. Flash-Speicher usw.) und/oder andere elektronisch lesbare Speichermedien umfassen. Der elektronische Speicher **419** kann eine oder mehrere virtuelle Speicherressourcen (z. B. Cloud-Speicher, ein virtuelles privates Netzwerk und/oder eine oder mehrere andere virtuelle Speicherressourcen) umfassen. Der elektronische Speicher **419** kann Softwarealgorithmen, vom Prozessor **420** ermittelte Informationen, von dem einen oder den mehreren Servern **401** empfangene Informationen, von der einen oder den mehreren Client-Computerplattformen 414/415 empfangene Informationen und/oder andere Informationen speichern, die dem einen oder den mehreren Server **401** erlauben, wie hierin beschrieben zu arbeiten.

[0134] Der Prozessor **420** kann konfiguriert sein, um Informationsverarbeitungsressourcen in dem einem oder den mehreren Servern **401** bereitzustellen. Somit kann der Prozessor **420** einen oder mehrere eines digitalen Prozessors, eines analogen Prozessors, ei-

ner digitalen Schaltung zum Verarbeiten von Information, einer analogen Schaltung zum Verarbeiten von Information, einer Zustandsmaschine und/oder anderer Mechanismen zum elektronischen Verarbeiten von Information umfassen. Obwohl der Prozessor **420** in **Fig. 1** als eine einzige Einheit gezeigt ist, dient dies nur der Veranschaulichung. In einigen Implementierungen kann der Prozessor **420** eine Mehrzahl von Verarbeitungseinheiten umfassen. Diese Verarbeitungseinheiten können physisch innerhalb derselben Vorrichtung angeordnet sein, oder der Prozessor **420** kann eine Verarbeitungsfunktionalität einer Mehrzahl von Vorrichtungen repräsentieren, die koordiniert arbeiten. Der Prozessor **420** kann für maschinenlesbare Befehle und/oder Komponenten von maschinenlesbaren Befehle durch Software; Hardware; Firmware; eine Kombination aus Software, Hardware und/oder Firmware; und/oder andere Mechanismen zum Konfigurieren von Verarbeitungsressourcen auf dem Prozessor **420** konfiguriert sein. Wie hierin verwendet, kann sich der Ausdruck „Komponente“ auf jede Komponente oder jeden Satz von Komponenten beziehen, die die der Komponente zugeordnete Funktionalität ausführen. Dies kann einen oder mehrere physische Prozessoren während der Ausführung von prozessorlesbaren Befehlen, den prozessorlesbaren Befehlen, Schaltungen, Hardware, Speichermedien oder andere Komponenten umfassen.

[0135] Der Client **414**/**415** und der Server **401** können Datenverarbeitungsressourcen umfassen, die unter Verwendung dedizierter Komponenten oder kundenspezifischer FPGA- oder ASIC-Schaltungen realisiert werden können. Diese Rechenressourcen sind geeignet, Software zu speichern und auszuführen, die Schritte des Verfahrens gemäß der vorliegenden Erfindung implementiert. Der zentrale Genehmigungsserver (**401**) verarbeitet Kunden-Registrierungsanfragen (**Fig. 1**), Kunden-Kryptowährungsadressen (**Fig. 2**), Kunden-Kontoaktualisierungsanfragen sowie Kryptowährungstransaktionen (**Fig. 3**). Der zentrale Genehmigungsserver (**401**) arbeitet somit mit einer Kunden-Informationsdatenbank (**404**) (z. B. Nutzer X: gesetzlicher Name, Geburtsdatum, Anschrift, Kontaktadresse, Anmeldeinformationen, Kryptowährungsadresse, Transaktionskriterien) sowie mit einer Transaktionsdatenbank (**413**) (z. B. Transaktion Y: Transaktions-ID, Kryptowährungsadressen des Senders und des Empfängers, Menge der übertragenen Münzen, Transaktionszeitpunkt und IP-Adresse des Kunden-Wallet des Senders und Empfängers) zusammen.

[0136] Rechtliche Identitäten von Besitzern für einzelne Währungsadressen sind in der Kunden-Informationsdatenbank gespeichert (**Fig. 1**, **Fig. 115**). Dies erfüllt die behördliche Anforderung „Know-Your-Customer“ und ermöglicht die Nutzung des Systems als Zahlungssystem für kommerzielle Aktivitäten. Diese Informationen sind jedoch für die Öffentlichkeit nicht zugänglich, um die pseudonyme Eigenschaft des CBEM und seines Transaktionsnetzwerks zu erhalten.

[0137] Wenn Münzen von jemandem gestohlen werden, können der oder die Diebstähle oder Hacker leicht ermittelt werden, indem die rechtliche Identität des einen oder der mehreren Empfänger aus der Kunden-Informationsdatenbank (**115**) abgerufen wird. Daher verhindert die Implementierung des Systems, dass Münzen des CBEM gestohlen werden.

[0138] Aufgrund der pseudonymen oder anonymen Natur von Bitcoin und alterativen Kryptowährungen, die auf der Bitcoin-Technologie basieren, ist das Münzguthaben einzelner Münzbesitzer nicht ermittelbar, indem nur die in der Blockchain gespeicherten öffentlichen Transaktionsdatensätze analysiert werden. Des Weiteren wird absichtlich, wenn man nur einen Teil der an einer bestimmten Währungsadresse verzeichneten Münzen ausgibt, die Menge nicht ausgegebener Münzen an einer neu erzeugten Währungsadresse verzeichnet. Durch die Analyse der Blockchain ist es für eine dritte Partei rechenintensiv zu verfolgen, wohin eine empfangene Summe von Münzen schließlich übertragen und an welcher Adressen sie verzeichnet wurde.

[0139] Mit der vorliegenden Erfindung ist eine Menge von Münzen, die einem gültig registrierten Nutzer gehört, durch das zentrale Leitungsorgan durch Analyse der Transaktionsdatensätze in der Transaktionsdatenbank (**413**) vollständig ermittel- und verfolgbar. Neben der Fähigkeit, einzelne Währungsadressen mit ihren Besitzern zu verknüpfen, wird diese einzigartige Eigenschaft des vorliegenden Systems durch die Verzeichnung nicht ausgegebener Münzen (falls vorhanden) an der Währungsadresse, von der die Münzen gerade gesendet/ausgegeben wurden, verbessert. Mit anderen Worten wird die Menge der an einer Währungsadresse verzeichneten Münzen erst dann Null, nachdem alle Münzen, die zuvor an diese Adresse gesendet wurden, gesendet/ausgegeben wurden (**322**). Diese einzigartige Eigenschaft vereinfacht nicht nur das Verfahren eines Drittanbieters zur Ermittlung und Verfolgung der Eigentumsübertragung von Kryptowährungsmünzen durch Analyse der Transaktionsdatensätze in der Blockchain, sondern ermöglicht auch Anwendungen des Systems für Finanz- und Bankaktivitäten, insbesondere solche, die von Dritten geprüft werden müssen.

[0140] Der zentrale Genehmigungsserver (**401**) kommuniziert mit einem oder mehreren Clients (414, 415), die Kunden-Wallets (**416**, **417**) implementieren. Ein Wallet kann operativ mit dem zentralen Genehmigungsserver (**401**) verbunden sein, um Daten zu senden oder zu empfangen, die sich auf eine Transaktion beziehen. Das Wallet kann in Software, Hard-

ware, online oder anderen geeigneten Mitteln implementiert sein. Das Wallet kann eine bestimmte Kryptowährung oder mehrere Kryptowährungsarten speichern.

[0141] Ein Nutzer eines Wallets fordert eine Transaktion an, die von einem oder mehreren zentralen Genehmigungsservern validiert werden muss (**401**). Daher sind die Clients über eine geeignete bidirektionale Datenübertragungsverbindung wie GSM, UMTS, DSL, Ethernet usw. mit den Servern (**401**) verbunden.

[0142] Die Erfindung kann Mittel umfassen, um verdächtige oder nicht autorisierte Transaktionen automatisch zu identifizieren und zu stoppen. Außerdem verhindert diese Erfindung, dass ein CBEM (i) für Geldwäsche verwendet wird und (ii) gestohlen wird. AML- und KYC-Richtlinien können von einer bestimmten Institution festgelegt werden oder mit festgelegten Regeln und Vorschriften übereinstimmen. Die vorliegende Erfindung ermöglicht somit, dass das CBEM und sein Transaktionsnetzwerk solche AML- und KYC-Richtlinien und -Vorschriften einhält. Zum Beispiel kann der PATRIOT OFFICER von GlobalVision Systems, ein fortschrittliches regelbasiertes intelligentes BSA/AML/ATF-System, zur effektiven Automatisierung des BSA/AML/ATF-Workflows durch Überwachung, Screening, Erfassung, Warnung, Untersuchung und Analyse verdächtiger Aktivitäten aller Transaktionen eingesetzt werden.

[0143] Gemäß einer Variante einer Ausführungsform oder Ausführungsformen der Erfindung kann eine Transaktion unter bestimmten Bedingungen verzögert oder gehalten und/oder rückgängig gemacht werden. Im Allgemeinen muss ein Sender eine Transaktion zum Zeitpunkt der Erstellung signieren. In einer Ausführungsform kann ein Nutzer eine Transaktion nicht rückgängig machen. Das Unternehmen, das das Transaktionsnetzwerk steuert, kann jedoch eine Transaktion (durch Halten der Transaktion, bis sie abläuft) auf Anforderung eines Nutzers effektiv „rückgängig machen“. In einer typischen Kryptowährung können Transaktionen nicht rückgängig gemacht werden. Bei dieser Variante der Erfindung jedoch hält das System eine Transaktion für eine Zeitspanne, z. B. eine vorbestimmte Zeitspanne, und wartet auf das Auftreten einer vorbestimmten Bedingung oder Bedingungen. Zum Beispiel kann ein Nutzer eine Transaktion erstellen, um CBEM an einen Verkäufer von Waren oder Dienstleistungen zu senden. In Reaktion auf eine Anfrage von dem Nutzer (Käufer) an das System, z. B. den zentralen Server, hält das System das Abschließen der Transaktion auf, bis eine vorbestimmte Zeit verstrichen ist. Wenn der Verkäufer innerhalb der vorgegebenen Frist akzeptable Waren oder Dienstleistungen liefert, wird der Käufer die Transaktion nicht wiederrufen. Wenn der Verkäufer innerhalb der vorgegebenen Zeit keine akzeptablen Waren oder Dienstleistungen liefert, kann der Käufer die Transaktion vor dem Ablauf der vorbestimmten Zeit abbrechen. Dies gibt dem Verkäufer einen Leistungsanreiz.

[0144] Eine Variante dieses Systems könnte die Zahlung bis zum und unter Vorbehalt des Erhalts einer Benachrichtigung von einem Dritten, z. B. einem Lieferdienst wie Federal Express®, UPS® oder DHL®, dass Waren transportiert oder geliefert wurden, durch den zentralen Server verzögern. Alternativ kann das Halten auch auf dem Transaktionsbetrag basieren. Zum Beispiel kann ein Nutzer automatisch ein Halten der Transaktion von einer Woche oder irgendeinem Zeitraum für irgendeine Transaktion oberhalb eines bestimmten Betrags festlegen wollen oder das System kann es Nutzern nur erlauben, Transaktionen zu halten, die höher als ein vorbestimmter Betrag sind. Das System kann auch eine maximale Haltezeit haben. Die maximale Zeitdauer des Haltens kann um einen vorbestimmten Zuwachs je einem zusätzlichen vorbestimmten Zuwachs des Transaktionsbetrags erhöht werden. Das Halten kann auch implementiert werden, basierend auf der Identifizierung von: (**1**) einer Transaktion, die aus einer riskanten Quelle stammt; (**2**) einer Partei, die in einer Sanktionsliste aufgeführt ist; (**3**) verdächtigen Aktivitäten eines Nutzers; (**4**) Mittel aus einer riskanten Quelle; (**5**) Mittel aus illegalen Quellen; 6) dem Überschreiten einer vorbestimmten Schwelle für eine Anzahl von erkannten verdächtigen Aktivitäten; (**7**) anderen geeigneten Bestimmungen.

[0145] In **Fig. 5** ist ein beispielhaftes Flussdiagramm für ein Halten gezeigt. In Schritt **511** erstellt ein Nutzer eine Transaktion zum Senden von X CBEM-Einheiten an einen Empfänger. In Schritt **502a** legt das System (die Steuereinheit, z. B. ein oder mehrere zentrale Server und/oder ein Smart Contract) eine Haltezeit für die Transaktion als Reaktion auf eine Nutzeranfrage und/oder automatisch fest, z. B. für ungewöhnlich große Transaktionen und/oder sich ungewöhnlich häufig wiederholende Transaktionen und/oder für andere verdächtige Transaktionen, wie an anderer Stelle hierin und/oder in Übereinstimmung mit staatlichen Vorschriften beschrieben ist. In Schritt **503** kann das System bestimmen, ob die spezifische Transaktion mit hinreichender Wahrscheinlichkeit Finanzkriminalität ist oder nicht. Wenn dies der Fall ist, macht das System in Schritt **504** die Transaktion rückgängig (z. B. durch Abbrechen oder Nicht-Genehmigen). In anderen Versionen kann der Nutzer die Transaktion abbrechen oder auf andere Weise rückgängig machen, beispielsweise aus den oben genannten Gründen (Waren oder Dienstleistungen, die nicht rechtzeitig geliefert wurden) und/oder aufgrund der Entdeckung von Finanzkriminalität. Die Transaktion wird daher nicht Teil des Ledgers, z. B. wird sie nicht veröffentlicht und auf der Blockchain oder dem Ledger aufgezeichnet.

[0146] Wenn in Schritt **503** keine Finanzkriminalität durch das System erkannt wird, ermöglicht das System bei Schritt **505** eine normale Veröffentlichung, Validierung und Bestätigung sowie das Aufzeichnen der Transaktion. Somit wird die Transaktion in Schritt **505** validiert und bestätigt. In Schritt 506 hat der Empfänger die CBEM-Einheiten in seinem/ihrem Konto. In einer weiteren optionalen Variante kann das System jedoch eine Finanzkriminalitäts-Transaktion erkennen und/oder auf sie hingewiesen werden und wenn dies der Fall ist, kann das System in Schritt **508** das Konto des Empfängers einfrieren. Wenn in Schritt **507** keine Finanzkriminalität vorliegt, wird der Empfänger in Schritt **509** die X CBEM-Einheiten zur Verwendung verfügbar haben, z. B. zum Senden an eine dritte Partei.

[0147] Am bevorzugtesten signiert ein Nutzer eine Transaktion in Schritt **501a** (Senden von X CBEM-Einheiten) und so kann der Nutzer selbst am bevorzugtesten eine Transaktion nicht rückgängig machen. Nur die Entität oder Partei, die das System steuert (der zentrale Server und/oder Smart Contract), kann eine Transaktion in Schritt **504** mit oder ohne Nutzergenehmigung rückgängig machen. In einer weiteren bevorzugten Version kann das System die Transaktion rückgängig machen, wenn der Nutzer wie oben erwähnt ein Halten für die Transaktion anfordert und wenn eine Bedingung (oder Bedingungen) nach einer bestimmten Zeit nicht erfüllt wurde (z. B. vom beabsichtigten Empfänger). In dieser Version verhält sich das System (der zentrale Server und/oder Smart Contract) wie ein automatischer Escrow-Agent (dt. „Hinterlegungsagent“).

[0148] In einigen Ausführungsformen kann ein Nutzer eine Transaktion rückgängig machen, z. B. wie folgt: der Smart Contract kann unter bestimmten Umständen und/oder in einigen Ausführungsformen des zentralen Servers ein Rückgängigmachen für einen begrenzten Zeitraum ermöglichen, indem der zentrale Server beim Erzeugen eines Mehrfachsignatur-Kunden-Wallets eine Mehrfachsignaturadresse erzeugt, die aus drei öffentlichen Schlüsseln erzeugt wird. In einigen der obigen Ausführungsformen werden zwei Schlüsselpaare (wobei jedes Paar einen öffentlichen Schlüssel und einen privaten Schlüssel aufweist) verwendet, wobei ein privater Schlüssel beim Kunden und ein privater Schlüssel beim zentralen Server liegt, um sicherzustellen, dass eine vom Kunden vorgeschlagene Transaktion zuerst die Genehmigung des zentralen Servers erhält, und können auch zum Kommunizieren des zentralen Servers mit dem Kunden, z. B. über das Kunden-Wallet, verwendet werden, wenn der Kunde eine Transaktion einleitet. Um diese Art von Verfahren weiter zu verwenden, jedoch dem Kunden die Möglichkeit zu geben, eine Transaktion rückgängig zu machen, besteht eine Möglichkeit darin, von zwei Schlüsselpaaren zu drei Schlüsselpaaren (d. h. drei Paaren aus privatem Schlüssel und öffentlichem Schlüssel) überzugehen. Die ersten beiden Schlüsselpaare können dieselben wie in der obigen Ausführungsform sein. Der Kunde würde auch über einen zusätzlichen privaten Schlüssel (und den entsprechenden öffentlichen Schlüssel in diesem dritten Schlüsselpaar) verfügen.

[0149] Der zentrale Server kann immer noch über ein oder mehrere Paare aus öffentlichem Schlüssel und privatem Schlüssel verfügen und der Kunde verfügt nun über zwei Paare aus öffentlichem Schlüssel und privatem Schlüssel. Man beachte, dass die Mehrfachsignaturadresse aus noch mehr Schlüsseln, wie beispielsweise vier öffentlichen Schlüsseln, erzeugt werden kann.

[0150] Die beiden privaten Schlüssel eines Kunden können in zwei separaten DAT-Dateien in demselben Wallet gespeichert werden. Der erste private Schlüssel zum Einleiten einer Transaktion kann wie üblich in einer Datei wallet.dat gespeichert werden. Der zweite private Schlüssel zum Bestätigen einer Transaktion kann in einer Datei confirm.dat gespeichert werden.

[0151] Ein Kunde kann den ersten privaten Schlüssel verwenden, um eine Transaktion zum Senden einer Summe von CBEM einzuleiten. Wenn es Zeit ist, die Zahlung zu bestätigen, und bevor eine Transaktion abläuft, kann der Kunde eine Bestätigungsschaltfläche drücken, um den zweiten privaten Schlüssel des Kunden zu verwenden, um die gleiche Transaktion zu signieren.

[0152] Alternativ kann das Kunden-Wallet so konfiguriert sein, dass es den zweiten privaten Schlüssel des Kunden verwendet, um die Transaktion gemäß einem Computerbefehl automatisch zu signieren (eine Transaktion z. B. eine Woche nach dem Einleitungszeitpunkt zu signieren). Der Kunde kann ein solches automatisches Verfahren stoppen oder pausieren, indem er auf eine Stopp/Pause-Schaltfläche klickt. Eine solche Transaktionsablaufzeit kann eine gewünschte Zeitspanne sein, indem eine Zeit gewählt wird, zu der die Transaktion unumkehrbar wird.

[0153] Beim Überwachen können, wie an anderer Stelle hierin beschrieben, Transaktionen gegen einen definierten Satz von Regeln (z. B. Gesetzen und/oder Vorschriften und/oder solchen von CBEM-Nutzern zur Regulierung oder Begrenzung von Transaktionen) überwacht werden, um verdächtige Transaktionen, z. B. Transaktionen, die an illegalen Aktivitäten wie Geldwäsche beteiligt sind, zu identifizieren, aufzuzeichnen und/oder zu melden (z. B. durch einen Bericht zu verdächtigen Tätigkeiten (SAR) und/oder einen Bericht zu verdächtigen Transaktionen (STR)). Wie in Verbindung mit **Fig. 5** erwähnt, können verdächtige Finanztransaktionen gehalten (Schritt **502a**) und/oder rückgängig gemacht werden (Schritt **504**).

[0154] Zum Beispiel kann das System verschiedene Formen von verdächtigen und/oder unangemessenen Aktivitäten in Bezug auf CBEM-Übertragungen und CBEM-Wallets erkennen. Ein Erfassungsverfahren kann das Bestimmen einer Risikobewertung basierend auf Folgendem umfassen:

1. Feststellen, wann Gelder aus riskanten und/oder illegalen Quellen stammen, z. B. indem Personen, die an irgendeiner Transaktion beteiligt sind, gegen eine oder mehrere Sanktionslisten wie eine No-Fly-Liste, eine Liste bekannter Terroristen, eine Liste mutmaßlicher Terroristen, Listen bekannter Geldwäscher, Listen sanktionierter Länder z. B. der USA, der Vereinten Nationen und/oder anderer ausgewählter Länder, Gelder, die von einer solchen verdächtigen Person oder Organisation kommen oder zu ihr gehen, und/oder Personen und/oder Organisationen, die an kriminellen Aktivitäten beteiligt sind, wie Kinderpornographie, Diebstahl anderer Kryptowährungen, Beteiligung an Cyberkriminalität usw. unter Verwendung ihrer überprüften Identitäten wie hier ermittelt abgeglichen werden.

2. Die Überwachung von Nutzern auf verdächtige Aktivitäten kann ferner eine Überwachung auf Grundlage der Transaktionsgröße, z. B. eines Transaktionswerts von mindestens einem bestimmten Betrag, z. B. 10.000 US-Dollar oder mehr, und/oder einer Häufigkeit von Transaktionen umfassen, z. B. Transaktionen, die sich auf mindestens einen bestimmten Betrag an gleiche und/oder verschiedene Währungsadressen innerhalb einer vorgegebenen Zeit summieren, z. B. in Summe mindestens 10.000 US-Dollar innerhalb eines Tages, beispielsweise basierend auf und in Entsprechung des Bank Security Act (BSA) und einen Währungstransaktionsbericht (CTR) ausgegebend. Andere Beispiele für verdächtige Transaktionen können beinhalten, woher ein Konto einen für das Konto ungewöhnlich großen Betrag erhält und/oder wohin es ihn überträgt und/oder ob eine Person oder Entität wegen verdächtiger Aktivitäten in der Vergangenheit erfasst wurde.

3. Eine Warnung und/oder Bewertung, die angibt, wie oft eine Person ihre anderen Kryptowährungen (nicht das CBEM dieser Anmeldung) außerhalb eines Wallets für das CBEM gemäß der Anmeldung gesendet hat.

4. Die Erfassung verdächtiger Aktivitäten kann auch die Verwendung von Webbrowsern umfassen, die verdächtige Aktivitäten überwachen können, indem sie eine Warnung für Websites senden, die von Regierungsbehörden oder assoziierten Parteien als hohes Risiko oder Bedrohung eingestuft werden.

[0155] In der vorliegenden Erfindung kann am bevorzugtesten ein Wallet, das in Verbindung mit dem CBEM der Anmeldung verwendet wird, auch jede Kryptowährung oder zumindest mehrere Formen von Kryptowährung empfangen, wie etwa die Original-Bitcoin-, Ether- und/oder Dash-Kryptowährung.

[0156] Wenn ein Nutzer beispielsweise ein Wallet in einer am meisten bevorzugten Ausführungsform hat und dieses Wallet für alle digitalen Währungstransaktionen verwendet, wird dieses Wallet mit dem zentralen Server (und/oder dem Smart Contract-Code) kommunizieren, so dass das System verdächtige Aktivitäten jenseits der Verwendung nur eines CBEM gemäß Ausführungsformen der Erfindung überwachen und erfassen kann. Als ein weiteres Beispiel kann eine Bank und/oder ein anderes Finanzinstitut ihre Kunden auffordern, Wallets gemäß der am meisten bevorzugten Ausführungsform zu verwenden, die Warnungen an eine Bank und/oder ein anderes Finanzinstitut erfassen und senden kann, wenn das System Transaktionen mit Nicht-System-Wallets und/oder Nicht-System-Kryptowährung erfasst.

[0157] Die Bewertung des Transaktionsrisikos, sei es eine AML-Risikobewertung und/oder eine andere Finanztransaktionsrisikobewertung, die hier oder anderweitig beschrieben wird, erfolgt in der Regel durch die Bestimmung von Risikobewertungen basierend auf Drittquellen basierend auf den hier beschriebenen Faktoren und anderen Faktoren. Die Financial Action Task Force zur Geldwäscherei (FATF) ist eine zwischenstaatliche Organisation, die Empfehlungen und Richtlinien für die Bekämpfung von Geldwäsche und Terrorismusbekämpfung gibt. Sie erstellt auch eine Liste von nicht-kooperativen Ländern oder Territorien, die meist als FATF-Blacklist bezeichnet wird. Die Bekämpfung der Finanzierung terroristischer Aktivitäten kann auch durch die Überwachung der IP-Adressen (**1**) zum Zeitpunkt der Registrierung der Nutzer; (**2**) zum Zeitpunkt der Erzeugung der Transaktionsadresse; und (**3**) zum Zeitpunkt des Einleitens einer Transaktion sowie durch Überwachen von Münz-Nutzungsmustern erreicht werden.

[0158] Eine spezielle Form der Geldwäsche, die vorzugsweise in die Überwachung und Ausgabe von Warnungen und Berichten einbezogen wird, ist das Waschen von Transaktionen. Transaktionswäsche ist eine Art von Geldwäsche, bei der es einem Händler möglich ist, Zahlungen zu erhalten (z. B. von angeblichen Kunden). Es muss keinen tatsächlichen Verkauf von Waren oder Dienstleistungen geben. Alternativ kann ein Unternehmen gegründet werden, das illegale Gegenstände (gestohlene oder gefälschte Waren, Waffen und/oder Drogen) verkauft und erhaltene Zahlungen verarbeitet, indem es solche Zahlungen an seriöse Online-Geschäfte weiterleitet, die scheinbar legitime Waren verkaufen. Transaktionswaschung ist heutzutage in Internet-Unternehmen

viel einfacher, die oft nicht die strengen KYC-Anforderungen erfüllen müssen. Die angeblichen legitimen Geschäfte können von überall auf der Welt über das Internet geführt werden. Aus diesen und anderen Gründen ist das Waschen von Transaktionen besonders schwierig zu stoppen. Zumindest bei dem CBEM der Ausführungsformen der vorliegenden Erfindung muss der Nutzer jedoch eine verifizierte Identität haben.

[0159] Warnungen oder Bewertungen, die aus von Drittquellen erzeugten Daten stammen, und/oder eine oder mehrere Softwarelösungen können verwendet werden. Vorhandene Softwarelösungen für die Finanztransaktions-Compliance können vorzugsweise Folgendes umfassen:

AML360, von AML360, Sydney, Australien, www.AML360software.com;

SafeWatch Profiling, von EastNets®, New York, NY, www.EastNets.com;

AML Manager, von Fiserv., Brookfield, Wisconsin, www.fiserv.com; und

[0160] Software, die sich mit AML-Geschäftsanforderungen befasst, kann Folgendes sowie andere Überwachung umfassen:

• Transaktionsüberwachungssysteme zur Identifizierung verdächtiger Transaktionsmuster, die zum Übermitteln von Berichten über verdächtige Aktivitäten (SARs) oder Berichten über verdächtige Transaktionen (STRs) führen können.

• Currency-Transaction-Reporting- (CTR) -Systeme zur Überwachung von Berichtsanforderungen für große Bartransaktionen (**10.000** US-Dollar und mehr in den USA).

• Kundenidentitätsmanagementsysteme zum Überprüfen und Überwachen verschiedener Negativlisten (z. B. OFAC), die einen ersten und fortlaufenden Teil der KYC-Anforderungen darstellen. Die elektronische Verifizierung kann auch gegen andere Datenbanken abgeglichen werden, um eine positive Bestätigung einer ID zu erhalten (in Großbritannien beispielsweise: das Wählerverzeichnis; die von Banken und Kreditagenturen verwendete „share“-Datenbank; Telefonlisten; Stromlieferantenlisten und Postzustelldatenbanken).

• Compliance-Software.

[0161] Eine zusätzliche Überwachung kann die Verifizierung der IP-Adresse oder -Adressen, die einem registrierten Nutzer zugeordnet sind, gegen eine oder mehrere Datenbanken von IP-Adressen im Zusammenhang mit Terrorismusfinanzierungstätigkeiten, Geldwäsche, Finanz-Geldwäsche und anderen illegalen Aktivitäten zu einer oder mehreren, vorzugsweise allen, der folgende Zeiten umfassen: zum Zeitpunkt der Nutzerregistrierung in dem System und/oder irgendeiner Nutzeraktualisierung, die zu einer Änderung der zugeordneten IP-Adresse oder -Adressen führt, periodisch zu vorbestimmten Zeitintervallen, zu einer Zeit der Erzeugung einer Transaktionsadresse, zu einer Zeit jeder vorgeschlagenen Transaktion oder Einleitung einer Transaktion und/oder zu einer Zeit, an der ein Transaktionsmuster ein vorbestimmtes Kriterium oder vorbestimmte Kriterien für verdächtige Aktivität erfüllt, und/oder zu irgendeiner Zeit, an der ein Schwellenrisiko in irgendeiner Hinsicht erreicht wird (bzgl. Transaktionsbetrag, Transaktion an eine verdächtige Person oder Organisation usw.).

[0162] Als weiteres Beispiel kann die IP-Adresse oder -Adressen des Nutzers darüber hinaus zum obigen Zeitpunkt überprüft werden, um zu erkennen, ob sich die Adresse oder Adressen in einem Land befinden, das unter Embargo und/oder Sanktionen steht, als Grundlage dafür, eine Transaktion zum Zeitpunkt der Transaktion rückgängig zu machen.

[0163] Die Überwachungssoftware kann Regeln umfassen, von und/oder in Verbindung mit:

•FinCEN - Financial Crimes Enforcement Network

•BSA - Bank Secrecy Act

•AML - Geldwäschebekämpfung

•SAR - Bericht über verdächtige Tätigkeiten

•RMLO - Residential Mortgage Loan Originator

•HIFCA - Region hoher Finanzkriminalitäts-Intensität

•HIDTA - Region hoher Drogenschmuggel-Intensität

•OFAC- Office of Foreign Assets Control

•Abteilungen des Finanzministeriums

- Financial Crimes Enforcement Network (FinCEN)

- Steuerverwaltung (IRS)

- Verbraucherschutzbüro (CFPPB)

- Staatliche Regulierungsbehörden

[0164] Einige oder alle Prüfungen zur Compliance mit Vorschriften und/oder andere Funktionen des zentralen Servers können durch den Quellcode in einem Smart Contract gesteuert werden.

1) Eine genehmigte Transaktionsadresse wird immer noch benötigt, aber in dieser Konfiguration kann es sich um eine Einzelsignatur- oder eine Mehrfachsignatur-Währungsadresse handeln.

2) Die genehmigte Währungsadresse, die der Identität des Kunden zugeordnet sein kann, wird wie zuvor beschrieben erzeugt.

3) Ein genehmigtes Transaktionsnetzwerk wird immer noch benötigt, aber in dieser Konfiguration wird die Genehmigungssteuerung erreicht, indem ein Smart Contract verwendet wird, um einige oder alle der gleichen Funktionen des oder der zentralen Server auszuführen, die bestimmte Eingaben oder Bedingungen erfordern, bevor sie eine Übertragung des CBEM erlauben.

4) Einige oder alle Steuer/Genehmigungsverfahren von Kunden/Nutzern und/oder von dem Leitungsorgan werden in den Smart Contract integriert.

[0165] Die Software, die den Distributed Ledger ausführt, wäre so programmiert, dass sie die signierte Transaktion empfängt und sie hält, z. B. bis verschiedene Bedingungen erfüllt sind, und sie dann aufzeichnet. Das Halten könnte vor oder nach Veröffentlichung und Validierung erfolgen. Eine Bedingung wäre, die Genehmigung des zentralen Servers zu erhalten.

[0166] Optional könnte der Smart Contract seine eigene Überprüfung der Risikobewertung oder die des zentralen Servers einleiten und wenn die Risikobewertung einen Schwellenwert erreicht oder überschreitet, könnte der Smart Contract die Transaktion verweigern. Der Smart Contract wäre im Wesentlichen ein Arm des zentralen Servers, da er nur einen Teil der Steuerung, die der zentrale Server bereits ausführt, auf die Software verlagern würde, auf der der Distributed Ledger ausgeführt wird.

[0167] Der folgende beispielhafte Arbeitsablauf kann verwendet werden.

[0168] Ein Nutzer leitet das Senden von CBEM durch Einleiten eines Smart Contract ein, gemäß dem ein Senden von CBEM eine Anzahl von Schritten durchläuft, die in dem Smart Contract voreingestellt sind, und ein gültiges Senden des CBEM erfordert die Erfüllung von Kriterien, die in dem Smart Contract voreingestellt sind.

[0169] Die Schritte und Kriterien, die in dem Smart Contract voreingestellt sind, können die folgenden chronologischen Ereignisse umfassen, z. B. wie in **Fig. 5** gezeigt. Ein weiteres Beispiel wäre das Halten einer Transaktion; das Überprüfen der Erfüllung verschiedener Bedingungen; Erfolg oder Misserfolg beim Abschluss des Smart Contracts (z. B. der Überprüfung der Risikobewertung durch den zentralen Server, der Genehmigung durch den zentralen Server); Erfolg; und Veröffentlichen im Netzwerk und Verifizieren und Aufzeichnen.

[0170] Um die Erfüllung verschiedener Bedingungen zu überprüfen, kann der Smart Contract entweder alle erforderlichen Arbeiten selbst ausführen oder mit dem zentralen Server zusammenarbeiten, um alle erforderlichen Arbeiten auszuführen. Im letzteren Fall dient der Smart Contract als Schnittstelle, um Anfragen an den oder die zentralen Server zu senden und Antworten von ihnen zu sammeln. Der Smart Contract verwendet dann die Antworten des oder der zentralen Server, um zu prüfen, ob alle erforderlichen Bedingungen erfüllt sind oder nicht. Der Smart Contract kann auch jede andere Quelle auf Erfüllung überprüfen, z. B. Drittquellen.

[0171] **Fig. 6** ist ein Flussdiagramm, das Komponenten eines AML- und Risikobewertungsmoduls zeigt, das das Verbinden mit verschiedenen Datenbanken mit relevanten Daten, das Analysieren von Transaktionen und vorgeschlagenen Transaktionen unter Verwendung von Daten von solchen Datenbanken zusammen mit Daten von der Identitätsdatenbank des vorliegenden Systems, Daten aus der Transaktionsdatenbank des vorliegenden Systems und Daten aus der vorgeschlagenen Transaktion (und/oder der überprüften Transaktion) und unter Verwendung von Compliance-Algorithmen, z. B. aus FATF-Anforderungen, das Bestimmen des Risikos und dann das Melden dieses Risikos falls benötigt/angefordert sowie das Ergreifen von oben genannten Maßnahmen von **Fig. 5** zum Halten oder Rückgängigmachen der Transaktionen umfasst. Wenn zum Beispiel der Nutzer eine Transaktion über das System vorschlägt (Schritt **501a** von **Fig. 5**), fordert das Wallet des Nutzers die Genehmigung der Transaktion vom zentralen Server an. Es kann ein Halten geben (Schritt 502a), während das System das Überwachen (Schritt **503**) gemäß **Fig. 6** und wie hierin beschrieben ausführt. In ähnlicher Weise kann, wenn das System wie in Schritt **507** überwacht, das in **Fig. 6** gezeigte und hierin beschriebene Verfahren befolgt werden. Der Compliance-Algorithmus, z. B. ein FATF-konformer Algorithmus, kann bestimmen:

- das KYC-Risiko durch die Identität des Kunden, die Empfängeridentität, den Standort (Land) des Kunden und Empfängers, aus Daten aus Beobachtungslisten und anderen externen Daten;

- das Transaktionsrisiko aus Fiat- und Blockchain-Transaktionsdaten und externen Daten;

- das interne Risiko durch Kundenidentität, Land des Kunden, Produktdaten und firmeninterne Daten; und

- das externe Risiko durch Gesetzgebung, Richtlinien, Medieninformationen und länderübergreifende Informationen.

[0172] Der Algorithmus verarbeitet die Eingabedaten und bestimmt ein Risikoniveau oder - Bewertung bezüglich der verschiedenen Risikoarten und kann

ein Signal, wie beispielsweise eine Warnung, an ein elektronisches Gerät (z. B. einen Computer eines Unternehmens-Compliance-Beauftragten) senden, z. B. durch Senden und Anzeigen auf dem Gerät, etwa einem Display auf seinem Monitor, und/oder durch eine akustische Warnung und/oder eine visuelle Warnung wie ein blinkendes Licht, falls eine Risikobewertung über einem vorbestimmten Schwellenwert liegt. Für verschiedene Arten von überwachten Risiken, z. B. AML, KYC, CTF, BSA und/oder FATF usw., können Schwellenwerte festgelegt werden. Das Gerät des Compliance-Beauftragten und/oder das System können automatisch einen SAR-, STR- und/oder anderen Bericht erstellen ihn automatisch an die eine oder mehreren zuständigen Behörden senden. Die Transaktion kann im Fall eines hinreichenden Risikos (das einen vorbestimmten Schwellenwert erreicht), bevor der zentrale Server die Genehmigung erteilt, nachdem die Genehmigung vom zentralen Server erteilt wurde und vor der Veröffentlichung im Netzwerk oder nach der Veröffentlichung und/oder nach der Validierung (obwohl nach der Validierung durch das Netzwerk es vorgezogen wird, die Transaktion nicht rückgängig zu machen), gestoppt, verzögert und/oder rückgängig gemacht werden. Der CBEM-Account des Empfängers, ebenso wie das Konto des Senders kann eingefroren werden, falls dies gerechtfertigt ist, und insbesondere für Transaktionen, die bereits validiert sind.

[0173] In anderen Ausführungsformen ist die Verwendung einer Mehrfachsignatur-Wallet-Adresse wünschenswert, egal ob das Wallet online oder offline gespeichert ist. Die Mehrfachsignatur ermöglicht es dem zentralen System, eine der M von N (z. B. zwei von drei) Signaturen darzustellen, die zum Signieren einer Transaktion erforderlich sind. Daher kann das System, wie an anderer Stelle hierin erwähnt, die vorgeschlagene Transaktion von einem Nutzer über das Mehrfachsignatur-Wallet empfangen, eine Finanztransaktionsüberwachung wie hierin erwähnt durchführen und die Transaktion signieren oder ihre Signatur zurückhalten, bis und falls kein signifikanter Verdacht auf verdächtige Aktivität oder ein anderes mit der Transaktion verbundenes finanzielles Risiko mehr besteht.

[0174] Das System kann z. B. dasselbe wie das in **Fig. 4** gezeigte oder ähnlich sein. Der Speicher **419** kann die Systembefehle enthalten, z. B. in einem nicht-flüchtigen Speicher. Der zentrale Genehmigungsserver 401 kann einen oder mehrere Monitore (graphische Nutzerschnittstellen), die mit ihm zur Anzeige wie hierin beschrieben verbunden sind, sowie jegliche Warnungen und/oder andere Warnmechanismen wie hierin beschrieben aufweisen. Der Speicher **419** kann auch hierin beschriebene Software zum Überwachen, Erfassen und/oder Warnen in Reaktion auf hierin beschriebene finanzielle Risiken und/oder Risikobewertungsbestimmungen umfassen. Die externen Ressourcen **418** können die verschiedenen Datenbanken, die benötigt werden, um Daten zur Verwendung bei der Berechnung des Risikos zu erhalten, und/oder externe Software umfassen, die bei der Berechnung des hierin genannten Risikos verwendet wird.

[0175] **Fig. 7** zeigt eine beispielhafte modifizierte Systemübersicht gemäß einer oder mehreren Implementierungen oder Varianten von **Fig. 4**, wobei eine verwendete Blockchain (oder ein Distributed Ledger) 700 und ein Smart Contract verwendet werden. Wie gezeigt, ist die verwendete Blockchain oder der Distributed Ledger mit einer Privatsphärenschicht **702** vorgesehen, die als Genehmigungsverwaltungsschicht für den Blockchain-Zugriff dienen kann. Sie kann beispielsweise auf einer Ethereum-Blockchain aufgebaut sein, z. B. der Blockchain **706** zur Verwaltung. Wie gezeigt, kann es einen Mechanismus für die Speicherung von Dateien geben (z. B. biometrische Daten und andere Dateien). Diese Elemente können mit einer Anwendungsprogrammierschnittstelle (API) **704** wie etwa einer Restful-API und z. B. einer Blockchain-Datenbank 708 zum Bereitstellen und/oder Verbessern der Speicherung, wie zum Beispiel BigChainDB, verbunden sein. Diese kann unter anderem mit einer biometrischen Applikation und einer Website verbunden sein. Andere Konfigurationen können verwendet werden. In dieser Ausführungsform kann die Verwaltung der Blockchain einen Smart Contract **707** umfassen. Tatsächlich kann die Blockchain **706** bei dieser Ausführungsform und bei einigen oder allen hier beschriebenen Ausführungsformen durch einen Distributed Ledger ersetzt werden. Ferner können in einigen oder allen Ausführungsformen andere Formen von verteiltem Speicher verwendet werden.

[0176] Wie in **Fig. 4** gezeigt, gibt es Client-Knoten **414**, **415** und es kann einen oder mehrere zentrale Server **401** geben, die eine Transaktionsdatenbank **413** und eine Kunden-Informationsdatenbank 115 umfassen können. Drittanbieterquellen und Out-of-Network-Partner 714 können die externen Ressourcen von **Fig. 4** aufweisen und können Out-of-Network-Knoten umfassen. Alle Systemkomponenten können über das Internet **720** kommunizieren. In einigen oder allen der obigen Ausführungsformen können die zentralen Serverfunktionen auf mehr als einen zentralen Server aufgeteilt sein. In einigen oder allen der obigen Ausführungsformen kann ein oder mehrere zentrale Server einem Kunden die Genehmigung erteilen, wenn der oder die zentralen Server dem Kunden Informationen über die Transaktion (wie etwa Informationen über die Verdächtigkeit der Transaktion/Wahrscheinlichkeit von Geldwäsche) übergegeben haben (genehmigte Transaktion), die der Kunde eingehen möchte. In anderen Ausführungsformen kann der oder die zentralen Server die Transaktion ablehnen. Wie an anderer Stelle hier-

in beschrieben, geschieht dies, indem eine automatische Genehmigung in Gegenwart einer oder mehrerer Bedingungen angefordert wird, die von dem oder den zentralen Servern bestimmt werden können. Eine spezielle Art und Weise, dies zu bewerkstelligen, ist die Verwendung eines Mehrfachsignatur-Wallets, bei dem der zentrale Server eine Transaktion, die der Client erstellt, signieren muss, bevor die Transaktion fortfahren kann. Eine andere Möglichkeit, wie diese Genehmigung für eine Transaktion erreicht werden kann, ist ein Verfahren, der als „Smart Contract“ bekannt ist. In einem Smart Contract bestimmen Computerbefehle, ob eine oder mehrere erforderliche Bedingungen für das Fortführen der Transaktion erfüllt sind. Tatsächlich werden einige oder alle Funktionen des oder der zentralen Server einfach durch Computerbefehle ausgeführt, die dem Quellcode der Software hinzugefügt werden, die auf einem Peer-to-Peer-Netzwerk ausgeführt wird, das die Blockchain steuert. Smart Contracts werden beispielsweise auf einem Server oder als dezentrale Applikation (auch als DApp bezeichnet) erzeugt. Eine DApp hat ein Frontend (in HTML) und ein Backend (im Wesentlichen eine Datenbank für das Frontend).

[0177] In einigen Implementierungen führt mindestens ein dedizierter Knoten das Signieren der Verifizierung der persönlichen Identität der ersten Person oder des ersten Nutzers durch. Ein bestimmter dedizierter Knoten kann einen oder mehrere Server umfassen. Der angegebene dedizierte Knoten kann ein öffentlicher Knoten oder ein privater Knoten sein, der zum Erstellen neuer Blöcke und/oder zum Signieren der Verifizierung konfiguriert ist.

[0178] In einigen Implementierungen kann das System von einem Systemverwaltungsdienstprogramm (SRU) oder einem Systemprozessor ausgeführt werden. Der Systemprozessor kann einen oder mehrere Server und/oder einen Smart Contract umfassen. Der Systemprozessor oder der oder die Server können konfiguriert sein, um mit einer oder mehreren Computerplattformen gemäß einer Client/Server-Architektur, einer Peer-to-Peer-Architektur und/oder anderen Architekturen zu kommunizieren. Die Nutzer können über Computerplattformen auf das System zugreifen. Der oder die Server und/oder der Smart Contract können zum Ausführen von maschinenlesbaren Befehlen konfiguriert sein. Die maschinenlesbaren Befehle können ein oder mehrere Systemverwaltungsdienstprogramme (SRU) und/oder andere Komponenten mit maschinenlesbaren Befehlen umfassen. Das SRU kann CBEM-Transaktionen empfangen und kann operativ mit dem verteilten Speicher, dem Distributed Ledger, der Blockchain oder einem anderen geeigneten verteilten Transaktionsmechanismus verbunden sein. Das SRU kann als ein Smart Contract und/oder als Computerbefehle auf dem oder den Servern implementiert sein und kann als von einem Systemprozessor ausgeführt betrachtet werden. Der Systemprozessor kann durch den Smart Contract, der zusammen mit einem zentralen Server arbeitet, oder nur einen zentralen Server oder nur einen Smart Contract gebildet werden.

[0179] Zwei Beispiele dafür, wie Warnungen und/oder Berichte verdächtiger Aktivitäten auftreten können, sind folgende: Beispiel A: Eine Summe von CBEM wird von einer Währungsadresse außerhalb unseres konformen Netzwerks an eine Währungsadresse in unserem konformen Netzwerk gesendet. Beispiel B: Eine Summe von CBEM wird von unserem konformen Netzwerk an eine Währungsadresse außerhalb unseres konformen Netzwerks gesendet.

[0180] In Beispiel A kann der zentrale Server als Reaktion auf die Erfassung eine oder alle der folgenden Aktionen ausführen:

1. Durchführung einer obligatorischen AML-Überprüfung (retrospektive Transaktionsanalyse);

2. Warnen des Nutzers (Kunden), dass das System den Empfang einer Summe von CBEM von außerhalb des konformen Netzwerks erkannt hat;

3. Der Nutzer oder Kunde kann wählen, einen Analysebericht des mit der Transaktion verbundenen AML-Risikos zu erhalten (z. B. zu kaufen) ; und/oder

4. Das System stellt eine entsprechende Flagge oder eine entsprechende Kennung für diese bestimmte CBEM-Summe bereit und verknüpft auch das Analyseergebnis des Systems mit (i) dem Ursprung der CBEM-Summe und (ii) vorherigen Transaktionen, die der Währungsadresse des Senders zugeordnet sind.

[0181] In Beispiel B kann das System zu dem Zeitpunkt, an dem der Nutzer oder Kunde eine Transaktions- (Sende-) Anfrage macht, eine Warnnachricht an diesen Nutzer ausgeben, die den Nutzer informiert, dass er eine Summe an eine Währungsadresse sendet, die außerhalb des konformen Netzwerks liegt. Es kann auch eine Option für den Nutzer geben, die AML-Prüfung des Systems (eine retrospektive Transaktionsanalyse) zu verwenden, um das AML-Risiko der beabsichtigten Empfängerwährungsadresse zumindest teilweise basierend auf den der Empfängerwährungsadresse zuvor zugeordneten Transaktionen zu bewerten.

[0182] Das System kann dem Nutzer optional auch die Möglichkeit geben, eine zusätzliche Bestätigung bereitzustellen, bevor der Nutzer die Summe des CBEM senden kann. Diese zusätzliche Bestätigungsanforderung kann eine Warnmeldung über das Risiko umfassen, das mit einer solchen CBEM-Sendeaktion verbunden ist, beispielsweise:

(i) dass der Sender wahrscheinlich für die Folgen einer solchen Transaktion mit dem damit verbundenen AML-Risiko verantwortlich ist; und/oder

(ii) eine Bewertung des AML-Risikos, das mit der Adresse des beabsichtigten Empfängers verbunden ist, etwa niedrig, mittel oder hoch, wobei diese Bewertung z. B. nur bereitgestellt werden kann, wenn der Nutzer sich entscheidet, die AML-Prüfung des Systems zu kaufen.

[0183] Vorzugsweise ist in beiden Beispielen A und B die AML-Prüfung obligatorisch, aber der Nutzer kann wählen, zu zahlen, um den AML-Risikoanalysebericht zu erhalten, und/oder der zentrale Server kann automatisch einen SAR- oder STR- oder anderen Bericht für die betroffene Regierungsbehörde vorbereiten, wenn festgestellt wurde, dass der Sender (Beispiel A: der Bericht kann z. B. Senderwährungsadresse, seine früheren Transaktionen und Herkunft der CBEM-Summe enthalten) oder Empfänger (Beispiel B: der Bericht kann z. B. Empfängerwährungsadresse und seine früheren Transaktionen enthalten) mit illegalen Transaktionsaktivitäten assoziiert ist.

[0184] Für den Fachmann ist leicht erkennbar, dass das vorgenannte Verfahren zur persönlichen Identifizierung und Verifizierung durch ein oder mehrere Computerprogramme ausgeführt und/oder gesteuert werden kann. Solche Computerprogramme werden üblicherweise unter Verwendung der Rechenressourcen in einem Computergerät ausgeführt. Anwendungen werden auf einem nicht-flüchtigen Medium gespeichert. Ein Beispiel eines nicht-flüchtigen Mediums ist ein nicht-flüchtiger Speicher, beispielsweise ein Flash-Speicher, während ein Beispiel eines flüchtigen Speichers RAM ist. Die Computerbefehle werden von einem Prozessor ausgeführt. Diese Speicher sind beispielhafte Aufzeichnungsmedien zum Speichern von Computerprogrammen, die computerausführbare Befehle umfassen, die alle Schritte des computerimplementierten Verfahrens gemäß dem hier vorgestellten technischen Konzept ausführen.

[0185] Die Erfindung liefert ein nützliches Ergebnis, das in verbesserter Sicherheit und Rückverfolgbarkeit von Transaktionen liegt. Dieses Ergebnis ist auch konkret und greifbar, da statistische Messungen eine verbesserte Sicherheit und weniger Versuche von CBEM-Diebstahl zeigen. Somit liefert die Erfindung ein nützliches, konkretes und greifbares Ergebnis. Der Arbeits- oder Änderungsbeleg wird durch die Tatsache erfüllt, dass die durch die Mittel der vorliegenden Erfindung erzielte verbesserte Sicherheit Generationen von Mehrfachsignaturadressen und Pay-to-Script-Hash-Transaktionen und deren spezifische Modifikationen, Implementierungen und Anwendungen benötigt, wodurch mit Kryptowährungen verbundene Daten transformiert werden. Aufgrund eines spezifischen Implementierungsschemas ist die Idee nicht abstrakt.

[0186] Während die hier gezeigte Erfindung mit Bezug auf bestimmte bevorzugte Ausführungsformen gezeigt, beschrieben und definiert wurde, implizieren diese Referenzen und Beispiele der Implementierung in der vorstehenden Beschreibung keine Einschränkung der Erfindung. Es ist jedoch offensichtlich, dass verschiedene Modifikationen und Änderungen daran vorgenommen werden können, ohne vom breiteren Umfang des technischen Konzepts abzuweichen. Die gezeigten bevorzugten Ausführungsformen sind nur beispielhaft und nicht erschöpfend für den Umfang des hier vorgestellten technischen Konzepts.

[0187] Dementsprechend ist der Umfang nicht auf die in der Beschreibung beschriebenen bevorzugten Ausführungsformen beschränkt, sondern ist nur durch die folgenden Ansprüche begrenzt.

ZITATE ENTHALTEN IN DER BESCHREIBUNG

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

Zitierte Nicht-Patentliteratur

- Meiklejohn S. et al., University of California, San Diego, 2013), dass Hinweise auf Interaktionen zwischen Institutionen identifiziert werden können, indem die Struktur der Beteiligung von Bitcoin-Adressen beim empirischen Einkauf von Waren und Dienstleistungen analysiert wird [0008]

Schutzansprüche

1. System zum Überwachen und Beschränken von Transaktionen mit Kryptographie-basiertem elektronischem Geld (CBEM), wobei das System umfasst:
einen Systemprozessor (420 und/oder 707), der ein Systemverwaltungsdienstprogramm ausführt, das zum Verarbeiten von Kunden-Identitätsregistrierungen, Kunden-Währungsadressen und CBEM-Transaktionen eingerichtet ist zum:
- Kommunizieren mit einem Kunden-Wallet (416, 417), um eine oder mehrere genehmigte Währungsadressen des Kunden zu erzeugen;
- Genehmigen einer Anfrage zur Erzeugung einer oder mehrerer genehmigter Währungsadressen des Kunden;
- Kommunizieren mit dem Kunden-Wallet (416, 417), um eine oder mehrere genehmigte Transaktionen zu erzeugen;
- Genehmigen einer oder mehrerer Transaktionen, um eine Einheit des CBEM an eine Währungsadresse zu senden;
- Untersuchen einer Transaktion unter Verwendung von Transaktionskriterien, die von einem zentralen Leitungsorgan oder einem Kunden definiert werden; und
- Speichern von Transaktionsinformationen (414) in einer Transaktionsdatenbank (413);
wobei das System ferner umfasst:
eine oder mehrere genehmigte Währungsadressen;
ein genehmigtes Transaktionsnetzwerk;
eine Kunden-Informationsdatenbank (115), die kommunikativ mit dem Systemprozessor (420 und/oder 707) verbunden ist;
eine Transaktionsdatenbank (413), die kommunikativ mit dem Systemprozessor (420 und/oder 707) verbunden ist; und
mindestens ein Kunden-Gerät (414, 415), das mit einem Kunden-Wallet (416, 417) versehen ist;
wobei das mindestens eine Kunden-Gerät eingerichtet ist zum:
- Erlangen einer Genehmigung von dem Systemprozessor (420 und/oder 707), um eine oder mehrere genehmigte Währungsadressen zu erzeugen;
- Erlangen einer Genehmigung von dem Systemprozessor (420 und/oder 707), um eine oder mehrere genehmigte Transaktionen zu erzeugen, um eine Einheit des CBEM an die Währungsadresse eines Empfängers zu senden;
- Erstellen einer oder mehrerer genehmigter Transaktionen, um eine Einheit des CBEM an die Währungsadresse eines Empfängers zu senden, indem die Transaktion signiert wird; und
- wobei der Systemprozessor (420 und/oder 707) in Reaktion auf den Empfang der genehmigten Transaktion eingerichtet ist, die genehmigte Transaktion für eine Zeitspanne zu verzögern, bevor er seine Genehmigung für die Transaktion gibt, wobei die Genehmigung von einer Bestimmung abhängt, ob eine oder mehrere Bedingungen erfüllt sind oder nicht.

2. System nach Anspruch 1, wobei der Systemprozessor einen zentralen Server (420) umfasst.

3. System nach Anspruch 1 oder 2, wobei das System eingerichtet ist, zu bestimmen, ob eine oder mehrere erforderliche Bedingungen erfüllt sind, damit eine Transaktion fortfährt, indem Computerbefehle von einer dezentralen Applikation (DApp) verwendet werden.

4. System nach einem der vorhergehenden Ansprüche, wobei das System eingerichtet ist, zu bestimmen, ob eine oder mehrere erforderliche Bedingungen für eine Transaktion erfüllt sind, indem Computerbefehle von Software verwendet werden, die in einem Peer-to-Peer-Netzwerk ausgeführt wird.

5. System nach einem der Ansprüche 1 bis 4, wobei der Systemprozessor einen Prozessor umfasst, der unter Verwendung eines Smart Contract (707) gesteuert ist.

6. System nach einem der Ansprüche 1 bis 4, wobei der Systemprozessor einen zentralen Server und einen Prozessor aufweist, der durch einen Smart Contract (707) gesteuert ist.

7. System nach einem der Ansprüche 1 bis 6, wobei es mehrere Kunden gibt.

8. System nach einem der Ansprüche 1 bis 7, wobei der Systemprozessor ferner eingerichtet ist zum:
Erstellen eines persönlichen Kontos für einen Nutzer;
Verifizieren und Aufzeichnen von Informationen zur tatsächlichen persönlichen Identität, die von einem Kunden übermittelt wurde;
Aufzeichnen eines Identitätsverifizierungsnachweises, der von einem Kunden übermittelt wurden;
Aufzeichnen einer genehmigten Währungsadresse, die von einem Kunden erzeugt wurde;
Zuordnen und Speichern einer genehmigten Währungsadresse, Informationen zur persönlichen Identität und eines Identitätsverifizierungsnachweis eines Kunden in der Kunden-Informationsdatenbank; und
Aufzeichnen des Besitzes der mindestens einen Einheit des CBEM in einer Transaktionsdatenbank unter Verwendung einer Währungsadresse eines Kunden.

9. System nach einem der Ansprüche 1 bis 8, wobei sich die eine oder die mehreren Bedingungen auf ein Verdachtsniveau in Bezug auf die Compliance der Transaktion mit Transaktionskriterien beziehen, betreffend mindestens eines von AML, KYC, CTF, BSA und FATF.

10. System nach einem der Ansprüche 1 bis 9, wobei der Systemprozessor die Transaktion stoppt, wenn der Systemprozessor feststellt, dass ein erforderliches Verdachtsniveau vorliegt.

11. System nach einem der Ansprüche 1 bis 10, wobei der Systemprozessor in Reaktion auf das Verstreichen der vorbestimmten Zeitspanne ohne Erhalten einer Anzeige, dass mindestens eine oder mehrere Bedingungen erfüllt sind, die Transaktion stoppt.

12. System nach einem der Ansprüche 1 bis 11, wobei der Systemprozessor in Reaktion auf das Verstreichen der vorbestimmten Zeitspanne ohne Erhalten einer Anzeige von dem Kunden, dass die Transaktion abgebrochen werden soll, die Transaktion genehmigt.

13. System nach einem der Ansprüche 1 bis 12, wobei der Systemprozessor die Transaktion stoppt, wenn der Systemprozessor keine Anzeige empfängt, dass die mindestens eine oder mehreren Bedingungen innerhalb der Zeitspanne erfüllt sind.

14. System nach einem der Ansprüche 1 bis 13, wobei die Anzeige der einen oder mehreren Bedingungen durch den Systemprozessor von einem elektronischen Gerät eines Dritten empfangen wird.

15. System zum Überwachen und Beschränken von Transaktionen mit Kryptographie-basiertem elektronischem Geld (CBEM), wobei das System umfasst:
einen Systemprozessor (420 und/oder 707), der ein Systemverwaltungsdienstprogramm ausführt, das zum Verarbeiten von Kunden-Identitätsregistrierungen, Kunden-Währungsadressen und CBEM-Transaktionen eingerichtet ist zum:
- Kommunizieren mit einem Kunden-Wallet (416, 417), um eine oder mehrere genehmigte Währungsadressen des Kunden zu erzeugen;
- Genehmigen einer Anfrage zur Erzeugung einer oder mehrerer genehmigter Währungsadressen des Kunden;
- Kommunizieren mit dem Kunden-Wallet (416, 417), um eine oder mehrere genehmigte Transaktionen zu erzeugen;
- Genehmigen einer oder mehrerer Transaktionen, um eine Einheit des CBEM an eine Währungsadresse zu senden;
- Untersuchen einer Transaktion unter Verwendung von Transaktionskriterien, die von einem zentralen Verwaltungsorgan oder einem Kunden definiert werden; und
- Speichern von Transaktionsinformationen (414) in einer Transaktionsdatenbank (413);
wobei das System ferner umfasst:
eine oder mehrere genehmigte Währungsadressen;
ein genehmigtes Transaktionsnetzwerk;
eine Kunden-Informationsdatenbank (115), die kommunikativ mit dem Systemprozessor (420 und/oder 707) verbunden ist;
eine Transaktionsdatenbank (413), die kommunikativ mit dem Systemprozessor (420 und/oder 707) verbunden ist; und
mindestens ein Kunden-Gerät (414, 415), das mit einem Kunden-Wallet (416, 417) versehen ist;
wobei das mindestens eine Kunden-Gerät eingerichtet ist zum:
- Erlangen einer Genehmigung von dem Systemprozessor (420 und/oder 707), um eine oder mehrere genehmigte Währungsadressen zu erzeugen;
- Erlangen einer Genehmigung von dem Systemprozessor (420 und/oder 707), um eine oder mehrere genehmigte Transaktionen zu erzeugen, um eine Einheit des CBEM an eine Währungsadresse eines Empfängers zu senden;
- Erstellen einer oder mehrerer genehmigter Transaktionen, um eine Einheit des CBEM an die Währungsadresse eines Empfängers zu senden, indem die Transaktion signiert wird; und
wobei der Systemprozessor (420 und/oder 707) nach Empfang der genehmigten Transaktion und Validierung und Bestätigung der genehmigten Transaktion durch das Transaktionsnetzwerk und in Reaktion auf einen Empfang des CBEM im Konto des Empfängers eingerichtet ist, das Konto des Empfängers für die Übertragung von CBEM als Reaktion auf die Feststellung eines Verdachtsniveaus in Bezug auf die Einhaltung der Transaktionskriterien einzufrieren, die von einem zentralen Leitungsorgan oder einem Kunden festgelegt wurden.

16. System nach Anspruch 15, wobei der Systemprozessor einen zentralen Server (420) umfasst.

17. System nach Anspruch 15 oder 16, wobei das System eingerichtet ist, zu bestimmen, ob eine oder mehrere erforderliche Bedingungen erfüllt sind, damit eine Transaktion abläuft, indem Computerbefehle von einer dezentralisierten Anwendung (DApp) verwendet werden.

18. System nach einem der Ansprüche 15 bis 17, wobei der Systemprozessor eingerichtet ist, zu bestimmen, ob eine oder mehrere erforderliche Bedingungen erfüllt sind, damit eine Transaktion fortfährt, indem Computerbefehle von Software verwendet werden, die in einem Peer-to-Peer-Netzwerk ausgeführt wird.

19. System nach einem der Ansprüche 15 bis 18, wobei der Systemprozessor einen Prozessor umfasst, der unter Verwendung eines Smart Contract gesteuert ist.

20. System nach einem der Ansprüche 15 bis 18, wobei der Systemprozessor einen zentralen Server und einen Prozessor umfasst, der durch einen Smart Contract gesteuert ist.

21. System nach einem der Ansprüche 15 bis 20, wobei der Systemprozessor ferner eingerichtet ist zum:
Erstellen eines persönlichen Kontos für einen Nutzer;

Verifizieren und Aufzeichnen von Informationen zur tatsächlichen persönlichen Identität, die von einem Kunden übermittelt wurden;
Aufzeichnen von eines Identitätsverifizierungsnachweises, der von einem Kunden übermittelt wurde;
Aufzeichnen einer genehmigten Währungsadresse, die von einem Kunden erzeugt wurde;
Zuordnen und Speichern einer genehmigten Währungsadresse, Informationen zur persönlichen Identität und eines Identitätsverifizierungsnachweises eines Kunden in der Kunden-Informationsdatenbank; und
Aufzeichnen des Besitzes der mindestens einen Einheit des CBEM in einer Transaktionsdatenbank unter Verwendung einer Währungsadresse eines Kunden.

22. System nach einem der Ansprüche 15 bis 21, wobei der Systemprozessor die Transaktionen der Kunden auf verdächtige Transaktionen überwacht und wobei das mindestens eine Kriterium ein Kriterium ist, das mindestens eines von einem Finanzkriminalitätsrisiko, einem Terrorfinanzierungsrisiko, eines Risikos einer Transaktion in Verletzung einer staatlichen Sanktionsliste und eines Risikos von Transaktionswäsche anzeigt, wobei das genehmigte Transaktionsnetzwerk modifiziert werden kann, um jegliche Transaktionen abzulehnen, die nicht die zentralen Transaktionskriterien erfüllen, die in dem Systemprozessor gespeichert sind.

23. System nach einem der Ansprüche 15 bis 22, wobei die Transaktionskriterien von einem zentralen Leitungsorgan definiert werden, um verdächtige Transaktionen zu stoppen, die wahrscheinlich an illegalen Aktivitäten wie Geldwäsche beteiligt sind, und der Systemprozessor die genehmigte Transaktion stoppt und/oder eine Warnung in Reaktion auf das Erhalten eines Hinweises auf eine verdächtige Transaktion ausgibt.

24. System nach Anspruch 15 bis 23, wobei der Systemprozessor eine transaktionsbezogene und/oder eine empfängerbezogene Risikobewertung ermittelt und erhält und das mindestens eine Kriterium sich auf die Risikobewertung bezieht.

25. System nach Anspruch 24, wobei die Risikobewertung auf mindestens einem Vergleich von identitätsbezogener Information von mindestens einem Kunden in dem System mit einer Sanktionsliste, einer Analyse von mindestens früheren Transaktionen eines Kunden auf verdächtige Aktivität, einer Analyse der genehmigten Transaktion auf verdächtige Aktivitäten, einer Analyse zum Identifizieren von Transaktionswäsche und einer Analyse einer Quelle des CBEM des Kunden auf riskante und/oder illegale Quellen basiert.

26. System nach Anspruch 24 oder 25, wobei die Risikobewertung erhöht wird in Reaktion auf mindestens eines von (i) ein oder mehrere Male, in denen ein Kunde CBEM außerhalb der Kunden-Wallet in dem konformen Netzwerk gesendet hat, wobei der Systemprozessor überwacht, wann CBEM von außerhalb des konformen Netzwerks empfangen oder nach außerhalb des konformen Netzwerks gesendet wird, und (ii) wobei der Systemprozessor Daten bezüglich mindestens einer der vom Kunden besuchten Websites erhält, indem er den Webbrowser des Clients überwacht, und wobei die Risikobewertung auf einem Risiko von Betrug, einem Risiko von Finanzkriminalität und einem Risiko von Terrorismus im Zusammenhang mit den Websites basiert.

27. System nach einem der Ansprüche 15 bis 26, wobei der Systemprozessor genehmigte Transaktionen auf verdächtige Aktivität überwacht und die Risikobewertung und/oder Daten, die bei der Bestimmung die Risikobewertung verwendet werden, von einer Drittanbieterquelle erhält.

28. System nach einem der Ansprüche 15 bis 26, wobei das Kunden-Wallet ein Mehrfachsignatur-Wallet und/oder ein Wallet zum Verarbeiten von intelligenten Verträgen ist.

29. System nach einem der Ansprüche 15 bis 28, wobei das Kunden-Wallet ein Wallet ist, das zu anderen Zeiten als dem Erstellen der genehmigten Transaktion offline gespeichert wird.

30. System zur persönlichen Identifizierung und Verifizierung zum Überwachen und Beschränken von Transaktionen mit Kryptographie-basiertem elektronischem Geld (CBEM), wobei das System umfasst:
einen Systemprozessor (420 und/oder 707), der ein Systemverwaltungsdienstprogramm ausführt, das zum Verarbeiten von Kunden-Identitätsregistrierung, Kundenwährungsadressen, CBEM-Transaktionen eingerichtet ist zum:
- Kommunizieren mit einem Kunden-Wallet (416, 417), um eine oder mehrere genehmigte Währungsadressen des Kunden zu erzeugen;
- Genehmigen einer Anfrage zum Erzeugen einer oder mehrerer genehmigter Währungsadressen des Kunden;
- Kommunizieren mit dem Kunden-Wallet (416, 417), um eine oder mehrere genehmigte Transaktionen zu erzeugen;
- Genehmigen einer oder mehrerer Transaktionen, um eine Einheit des CBEM an eine Währungsadresse zu senden;
- Untersuchen einer Transaktion unter Verwendung von Transaktionskriterien, die von einem zentralen Leitungsorgan oder einem Kunden definiert werden; und
- Speichern von Transaktionsinformationen (414) in einer Transaktionsdatenbank (413); wobei das System ferner umfasst:
eine oder mehrere genehmigte Währungsadressen;

ein genehmigtes Transaktionsnetzwerk;
eine Kunden-Informationsdatenbank (115), die kommunikativ mit dem Systemprozessor (420 und/oder 707) verbunden ist;
eine Transaktionsdatenbank (413), die kommunikativ mit dem Systemprozessor (420 und/oder 707) verbunden ist; und
mindestens ein Kunden-Gerät (414, 415), das mit einem Kunden-Wallet (416, 417) versehen ist;
wobei das mindestens eine Kunden-Gerät eingerichtet ist zum:
- Erlangen einer Genehmigung von dem Systemprozessor (420 und/oder 707), um eine oder mehrere genehmigte Währungsadressen zu erzeugen;
- Erlangen einer Genehmigung von dem Systemprozessor (420 und/oder 707), um eine oder mehrere genehmigte Transaktionen zu erzeugen, um eine Einheit des CBEM an eine Währungsadresse eines Empfängers zu senden;
- Erstellen einer oder mehrerer genehmigter Transaktionen, um eine Einheit des CBEM an die Währungsadresse eines Empfängers zu senden, indem die Transaktion signiert wird; und
wobei der Systemprozessor (420, 707) in Reaktion auf den Empfang einer genehmigten Transaktion von dem Kunden-Gerät die Transaktion basierend auf den Transaktionskriterien untersucht und ein Verdachtsniveau für eine genehmigte Transaktion bestimmt, und wenn das Verdachtsniveau über einem vorgegebenen Schwellenwert liegt, welcher anzeigt, dass illegale Aktivitäten basierend auf vorbestimmten Regeln wahrscheinlich sind, der Systemprozessor die Transaktion verweigert, wobei das Verdachtsniveau zumindest teilweise auf Kundeninformationen in der Kunden-Informationsdatenbank, der Transaktionsdatenbank, den Transaktionsinformationen bezüglich der genehmigten Transaktion, den Kriterien, die von einem zentralen Leitungsorgan definiert sind, dem Standort des Kunden und dem Standort des Empfängers und externen Quellen bestimmt wird.

31. System nach Anspruch 30, wobei der Systemprozessor einen zentralen Server umfasst.

32. System nach Anspruch 30 oder 31, wobei das System eingerichtet ist, zu bestimmen, ob eine oder mehrere erforderliche Bedingungen erfüllt sind, damit eine Transaktion abläuft, indem Computerbefehle von einer dezentralisierten Applikation (DApp) verwendet werden.

33. System nach einem der Ansprüche 30 bis 32, wobei der Systemprozessor eingerichtet ist, zu bestimmen, ob eine oder mehrere erforderliche Bedingungen für eine Transaktion erfüllt sind, indem Computerbefehle von Software verwendet werden, die in einem Peer-to-Peer-Netzwerk ausgeführt wird.

34. System nach einem der Ansprüche 30 bis 33, wobei der Systemprozessor einen Prozessor umfasst, der unter Verwendung eines Smart Contract gesteuert wird.

35. System nach einem der Ansprüche 30 bis 34, wobei der Systemprozessor einen zentralen Server und einen Prozessor umfasst, der durch einen Smart Contract gesteuert wird.

36. System nach einem der Ansprüche 30 bis 35, wobei es mehrere Kunden gibt.

37. System nach einem der Ansprüche 30 bis 36, wobei der Systemprozessor ferner eingerichtet ist zum:
Erstellen eines persönlichen Kontos für einen Nutzer;
Verifizieren und Aufzeichnen von Informationen zur tatsächlichen persönlichen Identität, die von einem Kunden übermittelt wurden;
Aufzeichnen eines Identitätsverifizierungsnachweises, der von einem Kunden übermittelt wurde;
Aufzeichnen einer genehmigten Währungsadresse, die von einem Kunden erzeugt wurde;
Zuordnen und Speichern einer genehmigten Währungsadresse, Informationen zur persönlichen Identität und eines Identitätsverifizierungsnachweises eines Kunden in der Kunden-Informationsdatenbank; und
Aufzeichnen des Besitzes der mindestens einen Einheit des CBEM in einer Transaktionsdatenbank unter Verwendung der Währungsadresse eines Kunden.

38. System nach einem der Ansprüche 30 bis 37, wobei die von dem zentralen Leitungsorgan oder dem Kunden definierten Kriterien Kriterien umfassen, die sich auf Transaktionswäsche beziehen, und der Systemprozessor eine Transaktion ablehnt, wenn er feststellt, dass Transaktionswäsche wahrscheinlich ist.

39. System nach einem der Ansprüche 30 bis 38, wobei die von dem zentralen Leitungsorgan oder dem Kunden definierten Kriterien Kriterien umfassen, die sich auf eine an der Transaktion beteiligte Quelle des CBEM beziehen.

40. System nach einem der Ansprüche 30 bis 39, wobei der Systemprozessor Eingaben von der Transaktionsdatenbank und externen Quellen verwendet.

41. System nach einem der Ansprüche 30 bis 40, wobei die von dem zentralen Leitungsorgan oder dem Kunden definierten Kriterien Kriterien umfassen, die sich auf eine Sanktionsliste beziehen.

42. System nach den Ansprüchen 30 bis 41, wobei der Systemprozessor bestimmt, ob der Kunde oder Empfänger auf Websites zugegriffen hat, und die von dem zentralen Leitungsorgan oder dem Kunden definierten Kriterien Kriterien umfassen, die sich auf eine Art von Website beziehen, auf die zugegriffen wurde.

43. System zur persönlichen Identifizierung und Verifizierung zum Überwachen und Beschränken von Transaktionen mit Kryptographie-basiertem elektronischem Geld (CBEM), wobei das System umfasst:
einen Systemprozessor (420 und/oder 707), der ein Systemverwaltungsdienstprogramm ausführt, das zum Verarbeiten von Kunden-Identitätsregistrierung, Kundenwährungsadressen, CBEM-Transaktionen eingerichtet ist zum:
- Kommunizieren mit einem Kunden-Wallet (416, 417), um eine oder mehrere genehmigte Währungsadressen des Kunden zu erzeugen;
- Genehmigen einer Anfrage zur Erzeugung einer oder mehrerer genehmigter Währungsadressen des Kunden;
- Kommunizieren mit dem Kunden-Wallet (416, 417), um eine oder mehrere genehmigte Transaktionen zu erzeugen;
- Genehmigen einer oder mehrerer Transaktionen, um eine Einheit des CBEM an eine Währungsadresse zu senden;
- Untersuchen einer Transaktion unter Verwendung von Transaktionskriterien, die von einem zentralen Leitungsorgan oder einem Kunden definiert werden; und
- Speichern von Transaktionsinformationen (414) in einer Transaktionsdatenbank (413);
wobei das System ferner umfasst:
eine oder mehrere genehmigte Währungsadressen;
ein genehmigtes Transaktionsnetzwerk;
eine Kunden-Informationsdatenbank (115), die kommunikativ mit dem Systemprozessor (420 und/oder 707) verbunden ist;
eine Transaktionsdatenbank (413), die kommunikativ mit dem Systemprozessor (420 und/oder 707) verbunden ist; und
mindestens ein Kunden-Gerät (414, 415), das mit einem Kunden-Wallet (416, 417) versehen ist;
wobei das mindestens eine Kunden-Gerät eingerichtet ist zum:
- Erlangen einer Genehmigung von dem Systemprozessor (420 und/oder 707), um eine oder mehrere genehmigte Währungsadressen zu erzeugen;
- Erlangen einer Genehmigung von dem Systemprozessor (420 und/oder 707), um eine oder mehrere genehmigte Transaktionen zu erzeugen, um eine Einheit des CBEM an die Währungsadresse eines Empfängers zu senden;
- Erstellen einer oder mehrerer genehmigter Transaktionen, um eine Einheit des CBEM an die Währungsadresse eines Empfängers zu senden, indem die Transaktion signiert wird; und
wobei der Systemprozessor (420 und/oder 707) eingerichtet ist zum:
Erzeugen und Übertragen eines Warnsignals an ein elektronisches Gerät als Reaktion auf mindestens eines von (i) Senden eines CBEM von der ersten Art von Kunden-Wallet an eine zweite Art von Kunden-Wallet, wobei die zweite Art von Kunden-Wallet außerhalb des mit Finanzregulierung konformen Netzwerks liegt; und (ii) Empfangen eines CBEM, das sich von dem mit Finanzregulierung konformen CBEM unterscheidet, durch die erste Art von Kunden-Wallet.

44. System nach Anspruch 43, wobei der Systemprozessor einen zentralen Server umfasst.

45. System nach Anspruch 43 oder 44, wobei das System eingerichtet ist, zu bestimmen, ob eine oder mehrere erforderliche Bedingungen erfüllt sind, damit eine Transaktion abläuft, indem Computerbefehle von einer dezentralisierten Anwendung (DApp) verwendet werden.

46. System nach einem der Ansprüche 43 bis 45, wobei das System geeignet ist, zu bestimmen, ob eine oder mehrere erforderliche Bedingungen erfüllt sind, damit eine Transaktion fortfährt, indem Computerbefehle von Software verwendet werden, die in einem Peer-to-Peer-Netzwerk ausgeführt wird.

47. System nach einem der Ansprüche 43 bis 46, wobei der Systemprozessor einen Prozessor umfasst, der unter Verwendung eines Smart Contract gesteuert wird.

48. System nach einem der Ansprüche 43 bis 46, wobei der Systemprozessor einen zentralen Server und einen Prozessor umfasst, der durch einen Smart Contract gesteuert wird.

49. System nach einem der Ansprüche 43 bis 48, wobei es mehrere Kunden gibt.

50. System nach einem der Ansprüche 43 bis 49, wobei der Systemprozessor ferner eingerichtet ist zum:
Erstellen eines persönlichen Kontos für einen Nutzer;
Verifizieren und Aufzeichnen von Informationen zur tatsächlichen persönlichen Identität, die von einem Kunden übermittelt wurden;
Aufzeichnen eines Identitätsverifizierungsnachweises, der von einem Kunden übermittelt wurde;
Aufzeichnen einer genehmigten Währungsadresse, die von einem Kunden erzeugt wurde;
Zuordnen und Speichern einer genehmigten Währungsadresse, Informationen eines Identitätsverifizierungsnachweises und Anmeldeinformationen zur Verifizierung der Identität eines Kunden in der Kunden-Informationsdatenbank; und
Aufzeichnen des Besitzes der mindestens einen Einheit des CBEM in einer Transaktionsdatenbank unter Verwendung der Währungsadresse eines Kunden.

51. System nach einem der Ansprüche 43 bis 50, wobei der Systemprozessor genehmigte Transaktionen auf verdächtige Aktivitäten überwacht und wobei der Systemprozessor eine Warnung an einen Kunden und/oder eine Regierungsbehörde ausgibt, wenn eine verdächtige Aktivitäten festgestellt wird.

52. System nach einem der Ansprüche 43 bis 51, wobei der Systemprozessor als Reaktion auf den Empfang einer genehmigten Transaktion von dem Kunden-Wallet die genehmigte Transaktion unter Verwendung von Transaktionskriterien, die durch ein zentrales Leitungsorgan (501) und/oder einen Kunden (502) definiert werden, mit Compliance-Kriterien vergleicht und mindestens die genehmigte Transaktion stoppt, die genehmigte Transaktion für eine vorbestimmte Zeitspanne anhält, eine Warnung bezüglich der genehmigten Transaktion oder des Kunden ausgibt und/oder die genehmigte Transaktion an das zentrale Leitungsorgan und/oder den Kunden meldet.

53. System nach einem der Ansprüche 43 bis 52, wobei der Systemprozessor ein Verdachtsniveau feststellt, dass eine genehmigte Transaktion gegen mindestens eines von AML einschließlich Transaktionswäsche, KYC, CTF, BSA und FATF-Compliance verstößt.

54. System nach Anspruch 53, wobei das Verdachtsniveau auf einer Analyse einer Anzahl von Malen basiert, die ein Kunde Kryptowährungen außerhalb des Kunden-Wallets in dem konformen Netzwerk gesendet oder empfangen hat.

55. System nach einem der Ansprüche 43 bis 54, wobei (i) der Systemprozessor Kunden auf verdächtige Transaktionen überwacht und die vom zentralen Leitungsorgan oder Kunden definierten Kriterien eine Anzahl von Malen umfassen, in denen ein Kunde in verdächtige Transaktionen involviert war, und/oder (ii) der Systemprozessor bestimmt, ob der Kunde oder Empfänger auf Websites zugegriffen hat, und wobei die Kriterien, die von dem zentralen Leitungsorgan oder dem Kunden definiert werden, Kriterien in Bezug auf eine Art von Website umfassen, auf die zugegriffen wird.

56. System zur persönlichen Identifizierung und Verifizierung zum Überwachen und Beschränken von Transaktionen mit Kryptographie-basiertem elektronischem Geld (CBEM), wobei das System umfasst:
einen Systemprozessor (420 und/oder 707), der ein Systemverwaltungsdienstprogramm ausführt, das zum Verarbeiten von Kunden-Identitätsregistrierung, Kundenwährungsadressen, CBEM-Transaktionen eingerichtet ist zum:
- Kommunizieren mit einem Kunden-Wallet (416, 417), um eine oder mehrere genehmigte Währungsadressen des Kunden zu erzeugen;
- Genehmigen einer Anfrage zum Erzeugen einer oder mehrerer genehmigter Währungsadressen des Kunden;
- Kommunizieren mit dem Kunden-Wallet (416, 417), um eine oder mehrere genehmigte Transaktionen zu erzeugen;
- Genehmigen einer oder mehrerer Transaktionen, um eine Einheit des CBEM an eine Währungsadresse zu senden;
- Untersuchen einer Transaktion unter Verwendung von Transaktionskriterien, die von einem zentralen Leitungsorgan oder einem Kunden definiert werden; und
- Speichern von Transaktionsinformationen (414) in einer Transaktionsdatenbank (413);
wobei das System ferner umfasst:
eine oder mehrere genehmigte Währungsadressen;
ein genehmigtes Transaktionsnetzwerk;
eine Kunden-Informationsdatenbank (115), die kommunikativ mit dem Systemprozessor (420 und/oder 707) verbunden ist;
eine Transaktionsdatenbank, die kommunikativ mit dem Systemprozessor (420 und/oder 707) verbunden ist; und
mindestens ein Kunden-Gerät (414, 415), das mit einem Kunden-Wallet (416, 417) versehen ist;
wobei das mindestens eine Kunden-Gerät eingerichtet ist zum:
- Erlangen einer Genehmigung von dem Systemprozessor (420 und/oder 707), um eine oder mehrere genehmigte Währungsadressen zu erzeugen;
- Erlangen einer Genehmigung von dem Systemprozessor (420 und/oder 707), um eine oder mehrere genehmigte Transaktionen zu erzeugen, um eine Einheit des CBEM an die Währungsadresse eines Empfängers zu senden;
- Erstellen einer oder mehrerer genehmigter Transaktionen, um eine Einheit des CBEM an die Währungsadresse eines Empfängers zu senden, indem die Transaktion signiert wird; und
- wobei (i) der Systemprozessor (420 und/oder 707) eingerichtet ist, um Kunden auf verdächtige Transaktionen zu überwachen, und die von dem zentralen Leitungsorgan oder dem Kunden definierten Kriterien eine Anzahl von Malen umfassen, in denen ein Kunde in verdächtige Transaktionen involviert ist, und (ii) der Systemprozessor bestimmt, ob der Kunde oder Empfänger auf Websites zugegriffen hat, und wobei die Kriterien, die von dem zentralen Leitungsorgan oder dem Kunden definiert werden, Kriterien in Bezug auf eine Art von Website umfassen, auf die zugegriffen wird.

57. System nach Anspruch 56, wobei der Systemprozessor einen zentralen Server umfasst.

58. System nach Anspruch 56 oder 57, wobei das System eingerichtet ist, zu bestimmen, ob eine oder mehrere erforderliche Bedingungen erfüllt sind, damit eine Transaktion abläuft, indem Computerbefehle von einer dezentralisierten Applikation (DApp) verwendet werden.

59. System nach einem der Ansprüche 56 bis 58, wobei der Systemprozessor eingerichtet ist, zu bestimmen, ob eine oder mehrere erforderliche Bedin-

gungen für das Fortsetzen einer Transaktion erfüllt sind, indem Computerbefehle von Software verwendet werden, die in einem Peer-to-Peer-Netzwerk ausgeführt wird.

60. System nach einem der Ansprüche 56 bis 59, wobei der Systemprozessor einen Prozessor umfasst, der unter Verwendung eines Smart Contract gesteuert wird.

61. System nach einem der Ansprüche 56 bis 59, wobei der Systemprozessor einen zentralen Server und einen Prozessor umfasst, der durch einen Smart Contract gesteuert wird.

62. System nach einem der Ansprüche 56 bis 61, wobei es mehrere Kunden gibt.

63. System nach einem der Ansprüche 56 bis 62, wobei der Systemprozessor ferner eingerichtet ist zum:
Erstellen eines persönlichen Kontos für einen Nutzer;
Verifizieren und Aufzeichnen von Informationen zur tatsächlichen persönlichen Identität, die von einem Kunden übermittelt wurden;
Aufzeichnen eines Identitätsverifizierungsnachweises, der von einem Kunden übermittelt wurde;
Aufzeichnen einer genehmigten Währungsadresse, die von einem Kunden erzeugt wurde;
Zuordnen und Speichern einer genehmigten Währungsadresse, Informationen zur persönlichen Identität und eines Identitätsverifizierungsnachweises eines Kunden in der Kunden-Informationsdatenbank; und
Aufzeichnen des Besitzes der mindestens einen Einheit des CBEM in einer Transaktionsdatenbank unter Verwendung einer Währungsadresse eines Kunden.

Es folgen 7 Seiten Zeichnungen

Anhängende Zeichnungen

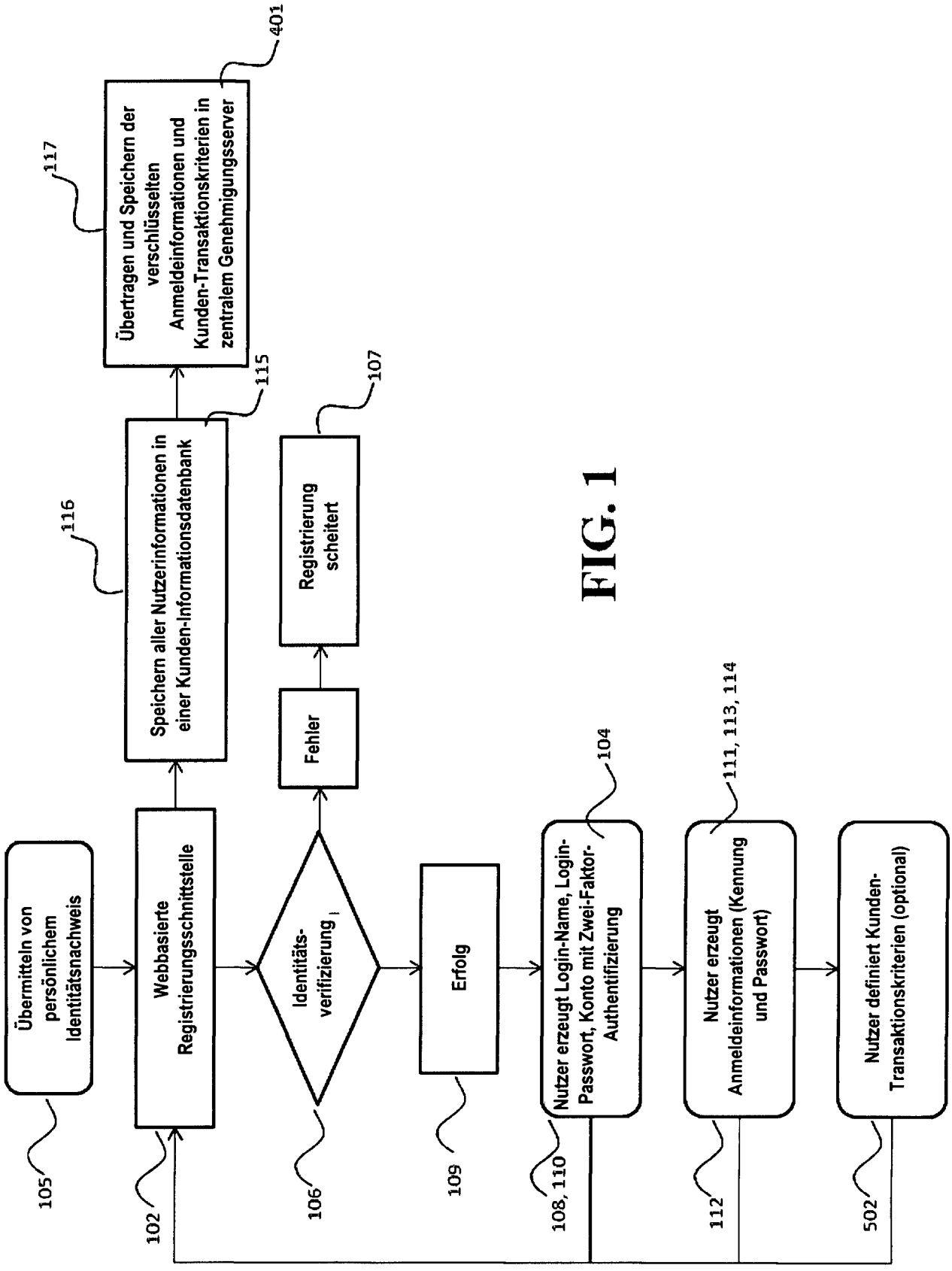


FIG. 1

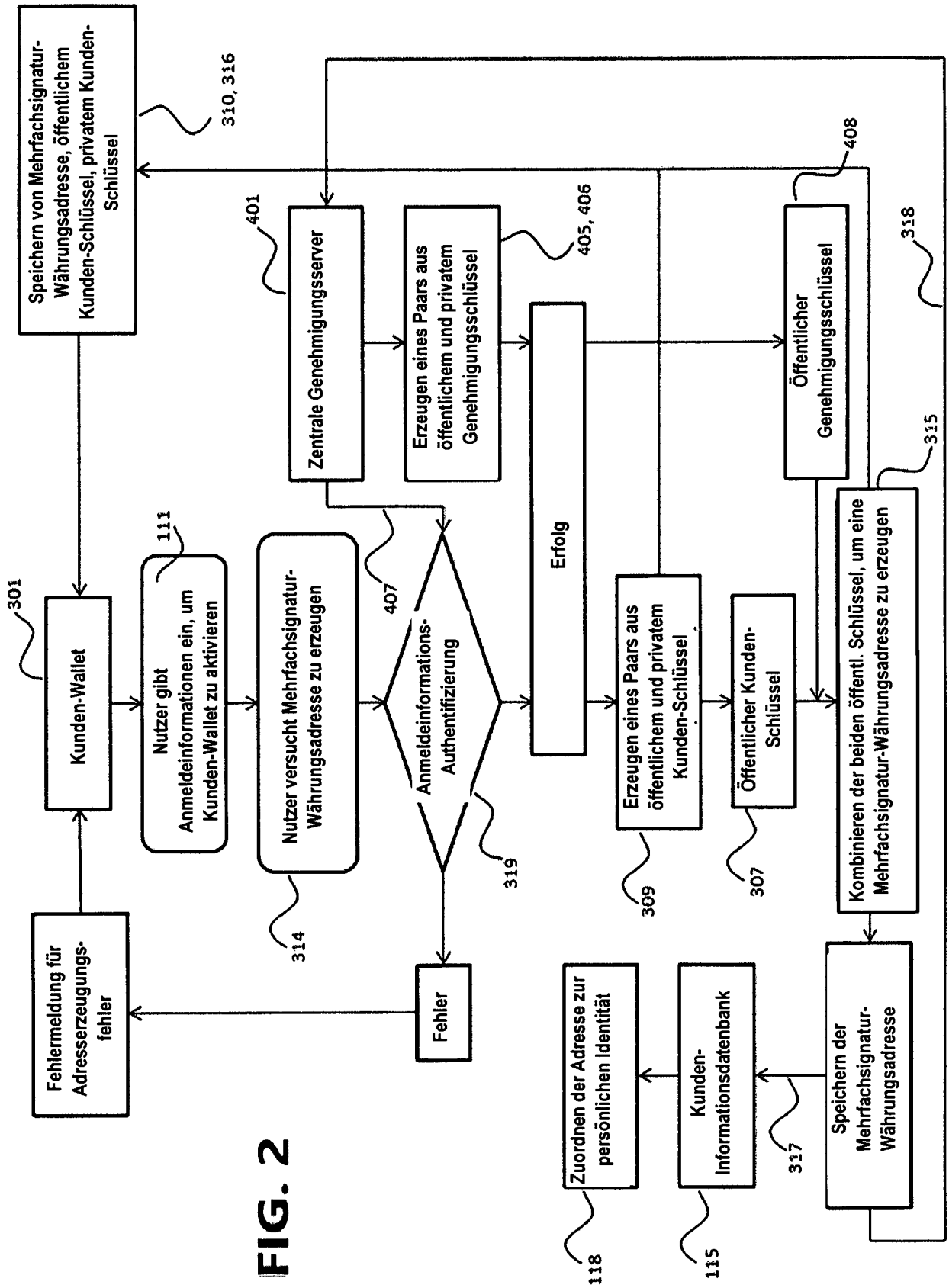
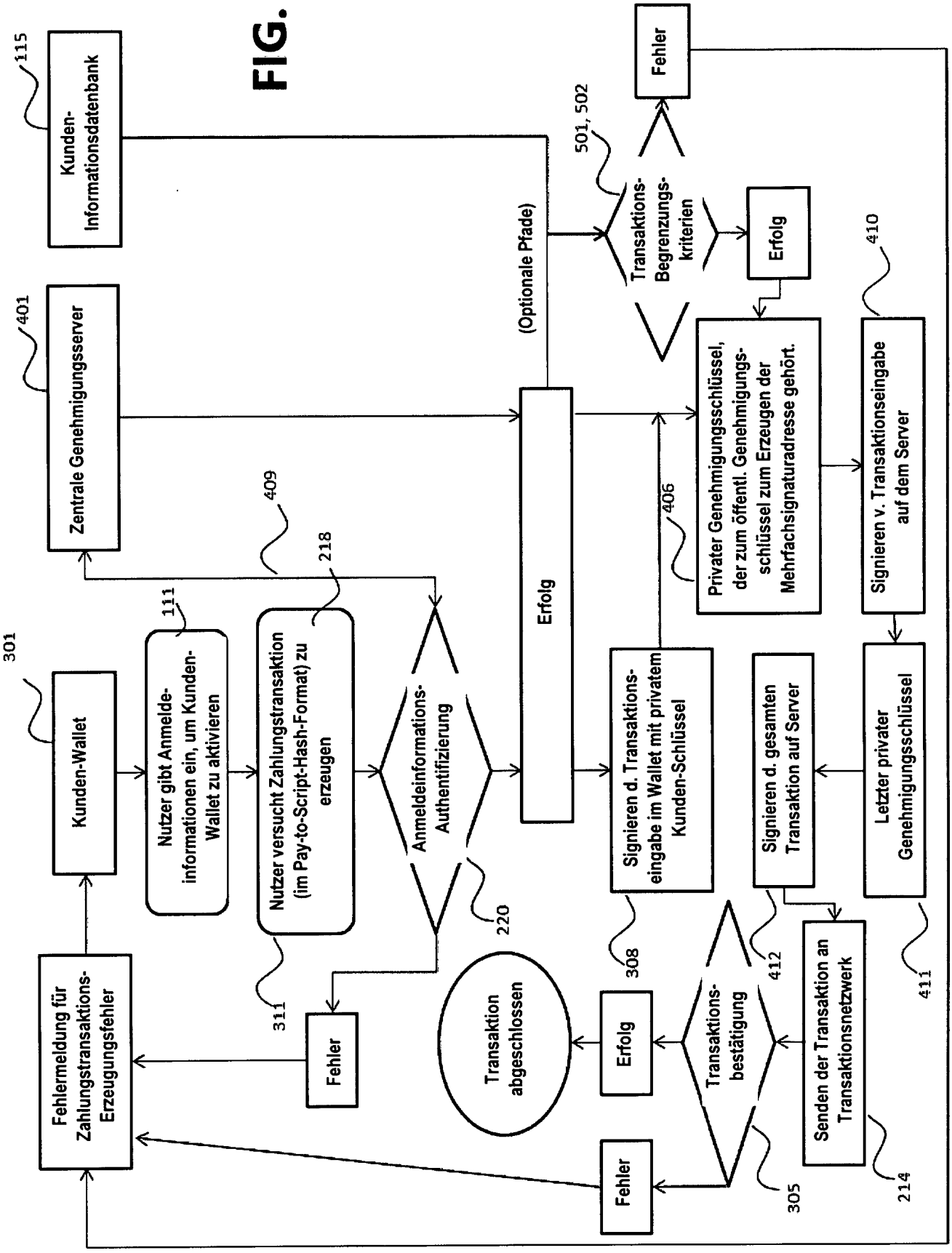

Speichern von Mehrfachsignatur-Währungsadresse, öffentlichem Kunden-Schlüssel, privatem Kunden-Schlüssel
310, 316
401
Zentrale Genehmigungsserver
Erzeugen eines Paars aus öffentlichem und privatem Genehmigungsschlüssel
405, 406
408
Öffentlicher Genehmigungsschlüssel
318
315
301
Kunden-Wallet
111
Nutzer gibt Anmeldeinformationen ein, um Kunden-Wallet zu aktivieren
Nutzer versucht Mehrfachsignatur-Währungsadresse zu erzeugen
407
Anmeldeinformations-Authentifizierung
319
Erfolg
Erzeugen eines Paars aus öffentlichem und privatem Kunden-Schlüssel
309
Öffentlicher Kunden-Schlüssel
307
Kombinieren der beiden öffentl. Schlüssel, um eine Mehrfachsignatur-Währungsadresse zu erzeugen
314
Fehlermeldung für Adresserzeugungs-fehler
Fehler
Zuordnen der Adresse zur persönlichen Identität
118
Kunden-Informationsdatenbank
115
317
Speichern der Mehrfachsignatur-Währungsadresse

FIG. 2

FIG. 3


115
Kunden-Informationsdatenbank
401
Zentrale Genehmigungsserver
301
Kunden-Wallet
111
Nutzer gibt Anmelde-informationen ein, um Kunden-Wallet zu aktivieren
218
Nutzer versucht Zahlungstransaktion (im Pay-to-Script-Hash-Format) zu erzeugen
409
Anmeldeinformations-Authentifizierung
220
Fehler
311
Fehlermeldung für Zahlungstransaktions-Erzeugungsfehler
(Optionale Pfade)
Erfolg
Signieren d. Transaktions-eingabe im Wallet mit privatem Kunden-Schlüssel
308
406
Privater Genehmigungsschlüssel, der zum öffentl. Genehmigungs-schlüssel zum Erzeugen der Mehrfachsignaturadresse gehört.
501, 502
Transaktions-Begrenzungs-kriterien
Fehler
Erfolg
410
Signieren v. Transaktionseingabe auf dem Server
Letzter privater Genehmigungsschlüssel
411
Signieren d. gesamten Transaktion auf Server
412
Transaktions-bestätigung
305
Fehler
Erfolg
Transaktion abgeschlossen
Senden der Transaktion an Transaktionsnetzwerk
214

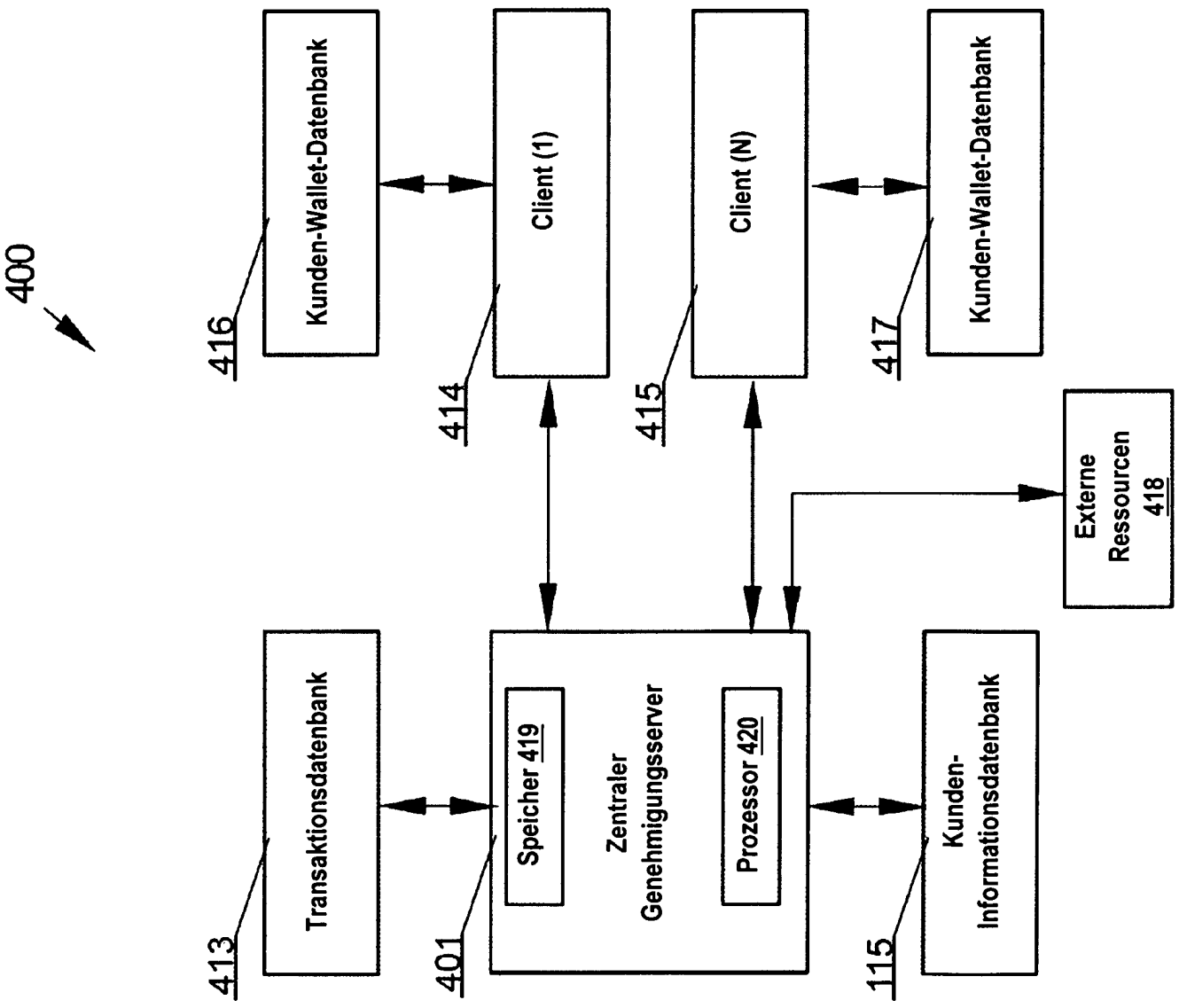
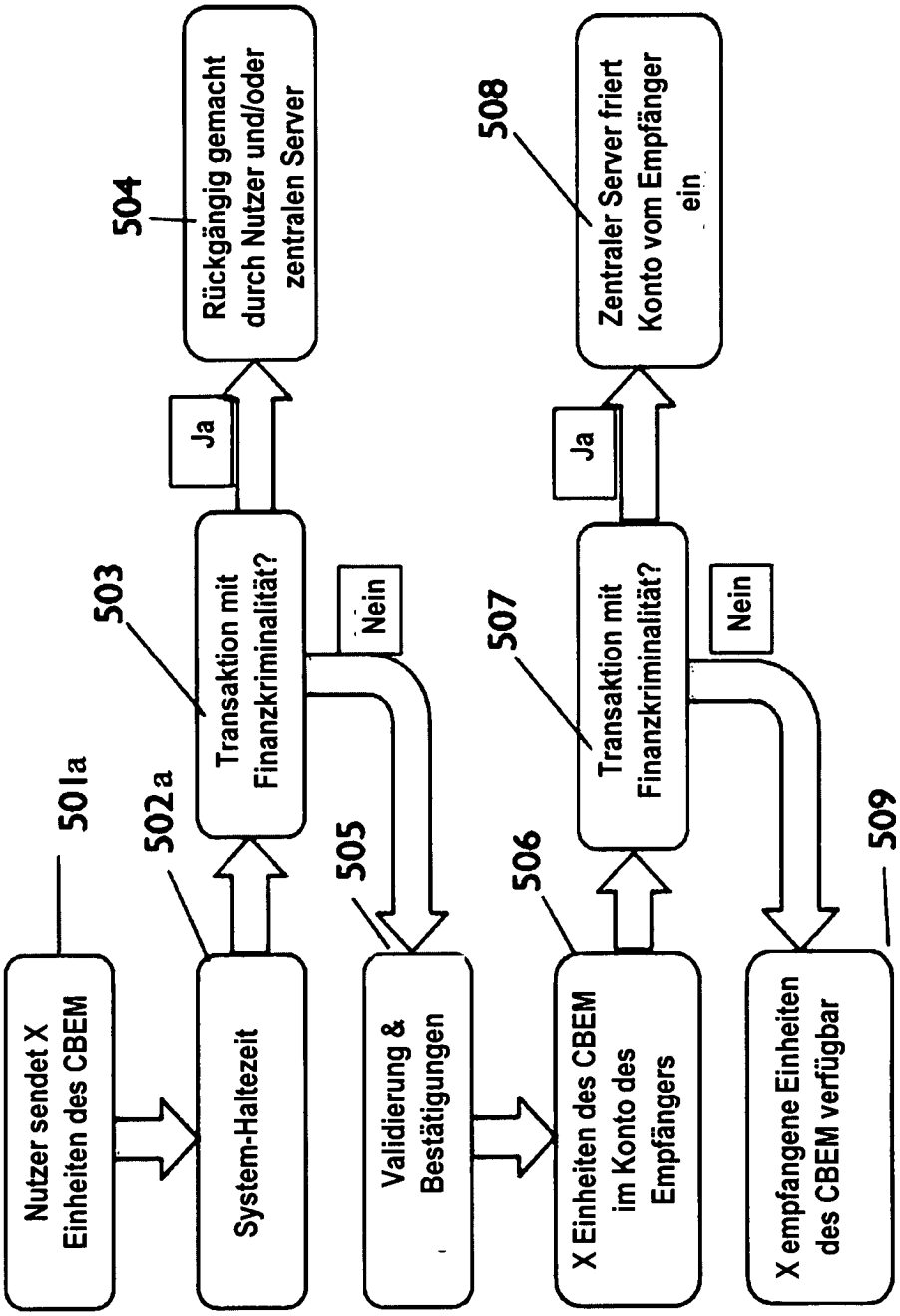

400
Kunden-Wallet-Datenbank
Client (1)
Client (N)
Kunden-Wallet-Datenbank
416
414
415
417
Externe Ressourcen 418
Transaktionsdatenbank
Speicher 419
Zentraler Genehmigungsserver
Prozessor 420
Kunden-Informationsdatenbank
413
401
115

Fig. 4

FIG. 5


Nutzer sendet X Einheiten des CBEM
501a
System-Haltezeit
502a
Transaktion mit Finanzkriminalität?
503
Ja
Rückgängig gemacht durch Nutzer und/oder zentralen Server
504
Nein
Validierung & Bestätigungen
505
X Einheiten des CBEM im Konto des Empfängers
506
Transaktion mit Finanzkriminalität?
507
Ja
Zentraler Server friert Konto vom Empfänger ein
508
Nein
X empfangene Einheiten des CBEM verfügbar
509

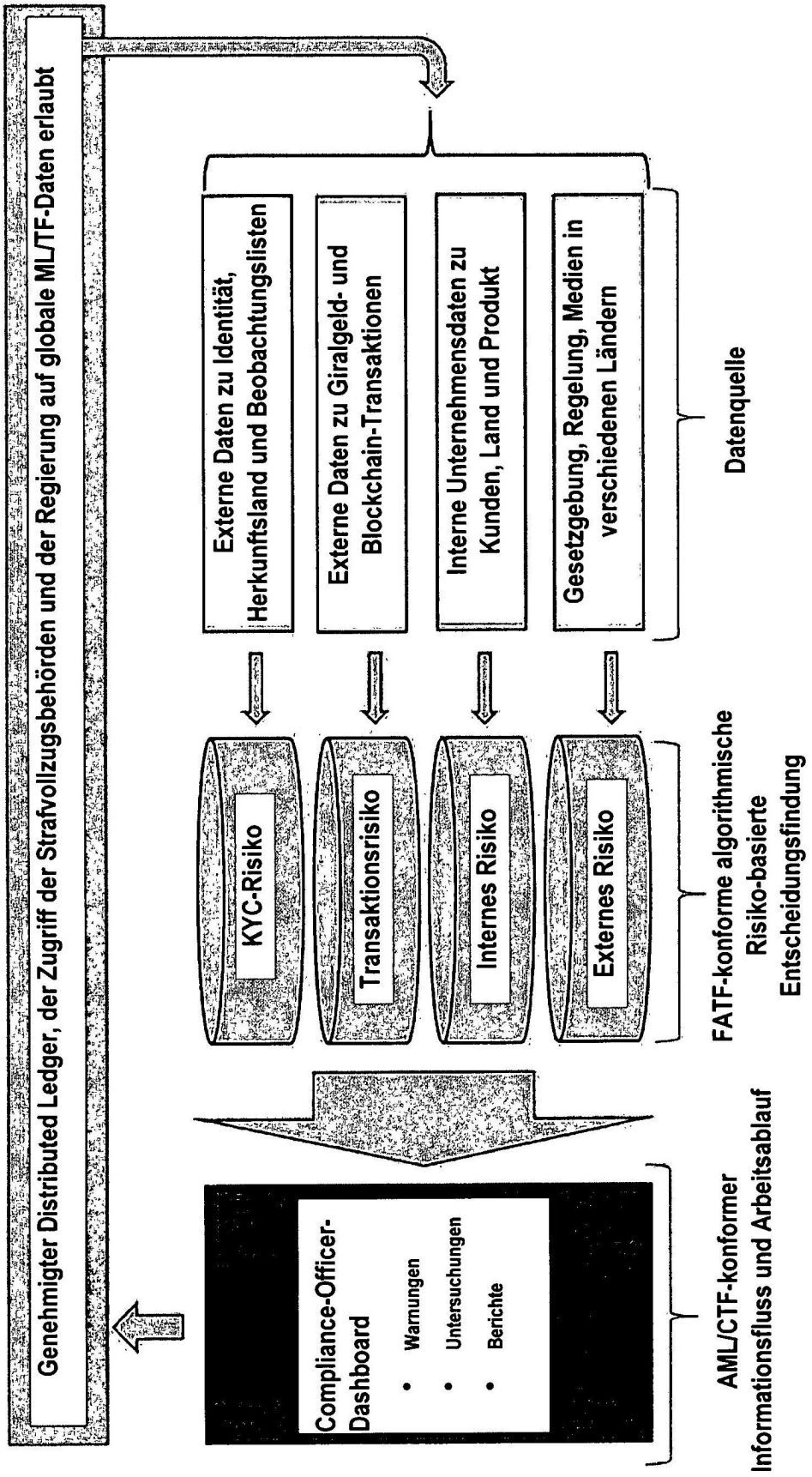

Genehmigter Distributed Ledger, der Zugriff der Strafvollzugsbehörden und der Regierung auf globale ML/TF-Daten erlaubt
Externe Daten zu Identität, Herkunftsland und Beobachtungslisten
Externe Daten zu Giralgeld- und Blockchain-Transaktionen
Interne Unternehmensdaten zu Kunden, Land und Produkt
Gesetzgebung, Regelung, Medien in verschiedenen Ländern
Datenquelle
KYC-Risiko
Transaktionsrisiko
Interes Risiko
Externes Risiko
FATF-konforme algorithmische Risiko-basierte Entscheidungsfindung
Compliance-Officer-Dashboard
Warnungen
Untersuchungen
Berichte
AML/CTF-konformer Informationsfluss und Arbeitsablauf

FIG. 6

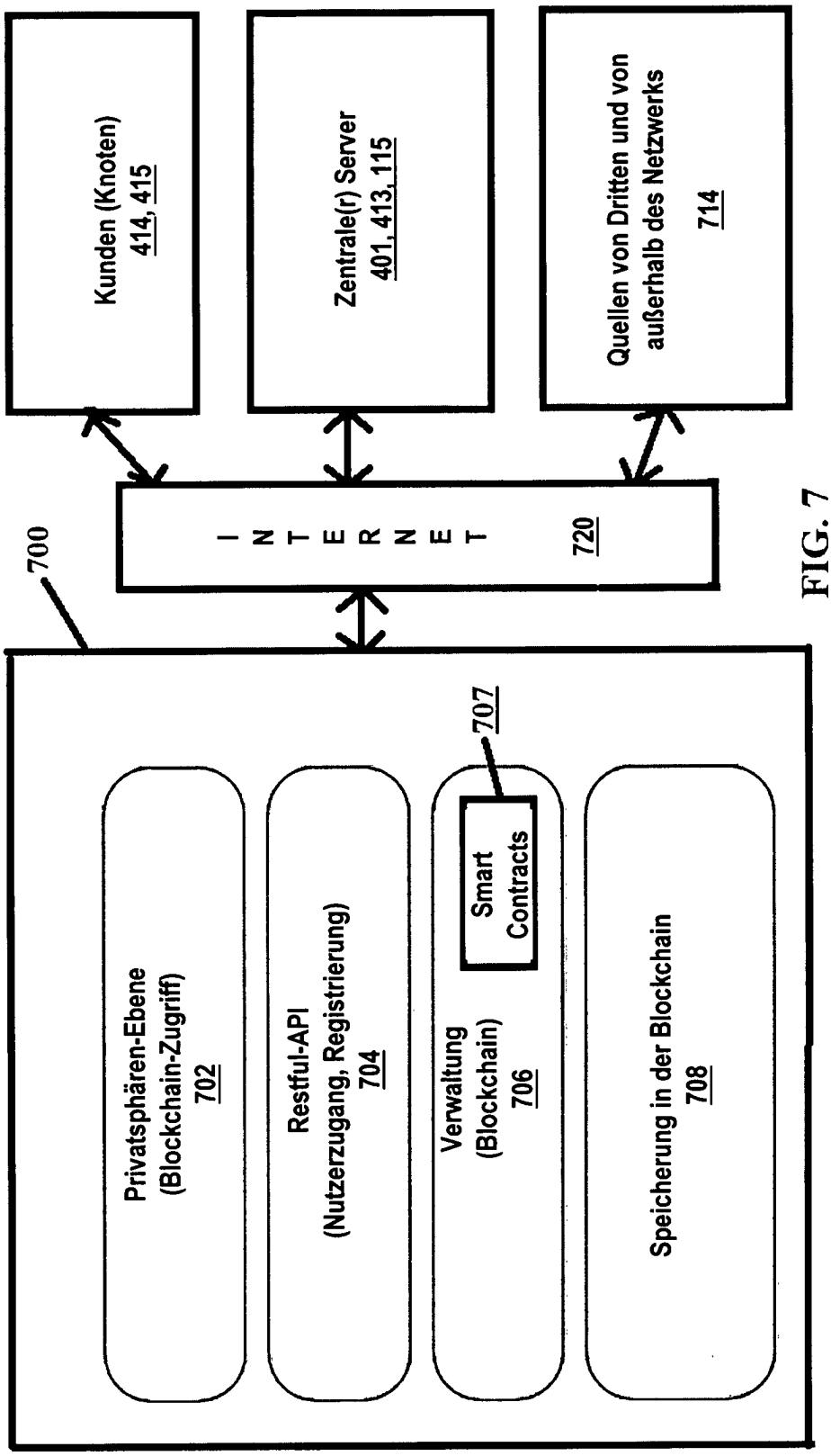

Kunden (Knoten)
414, 415
Zentrale(r) Server
401, 413, 115
Quellen von Dritten und von außerhalb des Netzwerks
714
INTERNET
720
700
Privatsphären-Ebene (Blockchain-Zugriff)
702
Restful-API (Nutzerzugang, Registrierung)
704
Verwaltung (Blockchain)
706
Smart Contracts
707
Speicherung in der Blockchain
708

FIG. 7