(19) Deutsches Patent- und Markenamt

(10) **DE 10 2018 000 228 A1** 2019.07.18

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2018 000 228.5**
(22) Anmeldetag: **15.01.2018**
(43) Offenlegungstag: **18.07.2019**

(51) Int Cl.: ***G06Q 40/00*** (2012.01)
G07F 19/00 (2006.01)

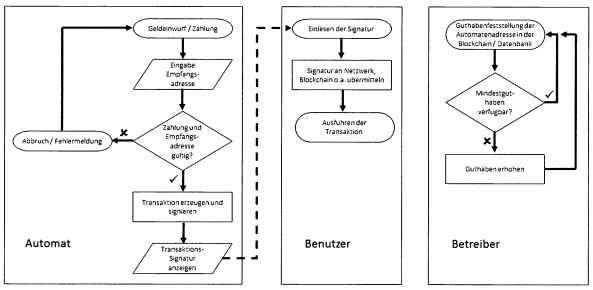
(71) Anmelder:
Hufeisen GmbH, 61231 Bad Nauheim, DE

(72) Erfinder:
Antrag auf Nichtnennung

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen.

(54) Bezeichnung: **Automat für kryptographische Gutscheine**

(57) Zusammenfassung: Herkömmliche Automaten, die kryptographische Coins oder Tokens ausgeben, sind entweder mit vorgefertigten Wallets bestückt, die Guthaben binden, oder sie benötigen eine Netzwerkanbindung, um die Coins oder Tokens an die Wallet des Kunden transferieren zu können.
Bei der Erfindung handelt es sich um einen Automaten zur Übertragung von kryptographischen Gutscheinen, in dem keine vorgefertigten Tokens, Paper Wallets o.ä. gespeichert sind und der ohne Anbindung an ein Datennetz auskommt und der dennoch per Fernwartung bestückt werden kann. Dazu ermittelt der Automat die kryptographische Empfangsadresse des Kunden und erzeugt die Signatur der bestellten Transaktion. Diese Signatur wird dem Kunden angezeigt, die dieser dann an das Netzwerk senden kann. Jede ausgeführte Transaktion kann der Automatenbetreiber von einem beliebigen, entfernten Ort aus feststellen und das Guthaben der Automatenadresse für den nächsten Verkauf auffüllen. So hält der Automat keine nennenswerten Guthaben vor und wird dennoch nie leer.
Der Automat kann zur Ausgabe von kryptographischen Coins oder Tokens verwendet werden, die als Bezahlgutscheine, Eintrittskarten, Fahrtausweise u.v.m. verwendet werden können. Wird das Prinzip in umgekehrter Weise angewendet, so dass der Automat keine Bezahlmittel annimmt, sondern Waren ausgibt und nicht der Automat die Tokens ausgibt, sondern der Kunde, entsteht ein Warenverkaufsautomat.
Das in der Zeichnung wiedergegebene Flussdiagramm macht unmittelbar ...



Beschreibung

[0001] Bei der Erfindung handelt es sich um einen Automaten zur Übertragung von kryptographischen Gutscheinen, in dem keine vorgefertigten Tokens, Paper Wallets o.ä. gespeichert sind und der ohne Anbindung an ein Datennetz auskommt und der dennoch per Fernwartung bestückt werden kann. Die kryptographischen Gutscheine können in Form von Einkaufsgutscheinen zum elektronischen Bezahlen, als Eintrittskarten, Fahrausweise o. a. verwendet werden.

Stand der Technik

[0002] Die folgenden Ausführungen setzen grundlegende Kenntnisse, so wie sie ein Fachmann auf diesem Gebiet besitzt, über die Funktionsweise von kryptographischen Währungen, Coins und Tokens, asymmetrischer Verschlüsselung, verteilter Datenbanken und der Blockchaintechnologie sowie der gebräuchlichen Terminologie voraus.

[0003] Die herkömmlichen Automaten, zum Beispiel Bitcoin-Automaten, funktionieren nach trivialen Prinzipien. Sie ziehen den Kaufpreis über eine Geldeingabeeinheit, etwa einen Münzeinwurf oder ein Banknotenlesegerät, ein. Daraufhin geben Sie den privaten Schlüssel einer mit kryptographischem Guthaben aufgeladenen Walletadresse aus. Da unterschiedliche Kryptowährungen und -tokens verschiedene Bezeichnungen verwenden, wird hier „Walletadresse“ für die Empfangsadresse verwendet, die meistens aus dem öffentlichen Schlüssel oder dessen Hash besteht. Entweder sind die Schlüssel bereits auf Papier gedruckt, das dann über den Warenschacht ausgegeben wird, oder das Ausdrucken erfolgt nach der Zahlung über einen eingebauten Drucker, oder der kryptographische Schlüssel wird auf einem Display zum Abscannen, meistens über einen als „QR-Code“ (eingetragenes Warenzeichen von Denso Wave Incorporated) bezeichneten, zweidimensionalen Binärmatrixcode angezeigt. Dies wird allgemein als „Paper Wallet“ bezeichnet. Der Käufer kann nun die Paper Wallet mittels einer speziellen Software über sein mobiles oder ein stationäres Gerät leeren („sweepen“) und das Guthaben in seine Wallet übertragen. Andere triviale Mechanismen, die eine Transaktion eigenständig an eine verteilte Datenbank, zum Beispiel an eine Blockchain (wie exemplarisch im US Patent 9,135,787 B1 beschrieben), oder an einen externen Dienst („3rd party“) zur Weiterverarbeitung senden (z. B. Korea Patent 1020160074178 A), sind in Herstellung, Betrieb und Wartung erheblich aufwändiger.

Mängel der bisherigen Ausführungen

[0004] Die bekannten Ausführungen lassen sich in mehrfacher Hinsicht verbessern. Bei den Ausführungen mit vorgefertigten Paper Wallets können die bereits ausgedruckten Wallets aus dem Automaten gestohlen werden. Außerdem müssen die Warenschächte regelmäßig neu befüllt werden. Das Anfertigen und Verpacken der Ausdrucke ist aufwändig. Auch bei den Varianten, die die Paper Wallets erst nach dem Bezahlvorgang drucken oder auf einem Bildschirm anzeigen, müssen die Paper Wallets mit den entsprechenden Guthaben im voraus bestückt werden, wodurch Vermögenswerte gebunden werden. Dieses Problem ließe sich durch ein Meldesystem lösen, das dem Betreiber mitteilt, welche Paper Wallets verkauft worden sind, damit diese dann umgehend mit Guthaben aufgeladen werden. Wenn die Paper Wallets nur eine zeitlich begrenzte Gültigkeit haben, kann die Meldung durch eine Blockchainabfrage ersetzt werden, die sichtbar macht, wieviele und welche Paper Wallets bereits gesweept wurden. Automaten, die Transaktionen an das Netzwerk senden, benötigen eine Anbindung an ein Intranet oder das Internet, wodurch sie Angriffen aus dem Netzwerk ausgesetzt sind („hot wallet“) und bei Ausfall der Netzwerkverbindung nicht mehr oder nur noch eingeschränkt funktionsfähig sind. Je nach Ausführung sind solche Automaten langsam bis sehr langsam, insbesondere, wenn Kryptowährungen mit langen Blockzeiten, wie Bitcoin, verkauft werden. Systeme, die eigenständig den Vorrat an kryptographischem Guthaben überwachen und bei Bedarf über externe Dienstleister, so genannten Exchanges, online auffüllen, müssen als Stand-alone-Gerät den API-Key gespeichert haben, mit dem sie sich gegenüber dem Exchange-Service zum Kauf von Cryptocoins, z. B. Bitcoins, als berechtigt ausweisen. Das Speichern des API-Keys im Automaten stellt ein Sicherheitsrisiko dar, weil ein Dieb oder Hacker, der in den Besitz des API-Keys gelangt, über das gesamte Guthaben des Betreibers bei der Exchange verfügen kann. Auch diese Geräte benötigen zum Funktionieren eine Anbindung an das Netzwerk, ebenso wie solche Varianten, die lediglich einen Auftrag zum Kaufen von kryptographischen Coins an eine Exchange weiterleiten (siehe WIPO 2015/134890 A1).

Lösung

[0005] Die benannten Mängel und Probleme werden durch die Erfindung beseitigt. Der Aufbau des Automaten ist trivial in der Hinsicht, dass er zum einen aus einem handelsüblichen Modul zum Empfang der Zahlung besteht, zum Beispiel einem Münzschacht, einem Geldscheinlesegerät, einem Kreditkartenleser, einem Bitcoin- (oder anderen Cryptocoins oder -tokens) Zahlungsanforderer oder anderen oder einer Kombination aus mehreren solcher Module. Zum anderen hat der Automat eine Ausgabeeinheit, zweckmäßigerweise einen scanbaren Bildschirm, über den auch Benutzungsanweisungen ausgegeben werden können. Auf das Zahlungs-, bzw. Geldeingabemodul kann verzichtet werden, wenn

Tokens kostenfrei ausgegeben werden sollen. Zu den herkömmlichen Systemen unterscheidet sich der Automat zum einen in der Funktion seiner Computereinheit, die einen weiteren Bestandteil des Automaten bildet. Sie braucht zur Erfüllung der Grundfunktion nicht an ein lokales Netzwerk oder das Internet angeschlossen zu sein. Der Kauf von kryptographischen Coins oder Tokens, unabhängig davon, ob diese als Zahlungsmittel, Einkaufs- oder Wertgutscheine, Eintrittskarten, Zugangsausweise, Reservierungsbestätigungen, Reisetickets oder anderem Verwendung finden, erfolgt, indem der Kunde, gegebenenfalls nach Durchlaufen einer vorbereitenden Prozedur wie Identifikation oder dem Quittieren von rechtlichen Hinweisen oder anderem, seine Zahlung in der vom Automaten angebotenen Form leistet. Sobald der Automat die Zahlung als gültig einstuft, zum Beispiel nach einer Echtheitsprüfung der eingegebenen Banknoten oder einem anderen Verfahren, muss der Kunde eine Wallet-Adresse, das ist in der Regel der Hashwert seines privaten Schlüssels, eingeben, die als Empfangsadresse fungiert. Hierzu sind viele Ausführungsvarianten denkbar. Eine manuelle Tastatureingabe erscheint wegen hoher Fehleranfälligkeit weniger zweckmäßig als das Abscannen eines Matrix- oder Barcodes, den der Kunde auf seinem Smartphone gespeichert haben kann, oder die Übertragung über NFC (near field communication) oder einen anderen maschinellen Weg. Der im Automaten eingebaute Scanner oder ein alternativer Datenempfangsmechanismus geben die vom Kunden eingegebene Walletadresse an die Computereinheit weiter, deren Software nun eine Transaktion von kryptographischen Einheiten an diese Adresse erzeugt und mit dem in der Computereinheit gespeicherten privaten Schlüssel der Walletadresse des Automatenbetreibers signiert. Die Signatur der Transaktion wird dem Kunden angezeigt, zum Beispiel in Form einer optisch scanbaren Binärmatrix. Nun kann der Kunde die Transaktion an das Netzwerk senden. Somit reicht es aus, in der Computereinheit lediglich den privaten Schlüssel zu speichern, der entweder durch geeignete Software oder Hardware gegen Diebstahl geschützt sein kann. Zum anderen ist die Computereinheit räumlich, logisch und/oder konstruktiv so von den Ein- und Ausgabemodulen, die für Kunden zugänglich sind, getrennt ist, dass die Computereinheit physisch und/oder deren Inhalt logisch nicht oder nur unter hohem Aufwand zu erreichen ist und/oder auf ihren Dateninhalt nicht von Unbefugten zugegriffen werden kann. Dadurch kann der Zugriff auf den privaten Schlüssel durch Unbefugte unterbunden werden. Zudem gehört der private Schlüssel zu einer Walletadresse, die nur geringes Guthaben aufweisen muss. Da jede Transaktion sofort in der Blockchain sichtbar wird und das abgezogene Guthaben von jedem Ort der Welt aus sofort, auch automatisiert, wieder aufgefüllt werden kann, sind Diebstahl und Manipulation zuungunsten des Betreibers praktisch unmöglich. Ein solcher Automat ist kostengünstig herzustellen, einfach zu bedienen, führt den gesamten Verkaufsvorgang schnell aus, ist sicher, muss nie vor Ort befüllt werden, benötigt keine Netzwerkanbindung, kann jede Form von physischen, elektronischen, virtuellen und sonstigen Zahlungsmitteln und -formen akzeptieren und jede Form von elektronischen und virtuellen Coins oder Tokens ausgeben. Außer der Entnahme des Bargelds benötigt der Automat keine Wartung. Wenn er mit Solarzellen, einer Handkurbel oder einer anderen elektrischen Inselversorgung betrieben wird, ist nicht einmal ein Anschluss an das Stromnetz erforderlich. Der Automat kommt ohne Anbindung an Server, an eine Blockchain oder andere verteilte Datenbanken oder Verzeichnisse aus und verzichtet gleichzeitig auf die Inanspruchnahme von Diensten Dritter; die Erfindung verletzt somit nicht das Peer-to-Peer-Prinzip! Die Grundausführung kann um Zusatzfunktionen erweitert werden, auch um solche, die Netzwerkanbindung verlangen, wie Kursabfragen, online Identifizierungen, Echtzeitkommunikation mit Kundenbetreuern, Sprachsteuerung, Anleitungen, Avatarfunktionen etc. Die für solche Zusatzfunktionen erforderliche Netzwerkanbindung muss dabei nicht zwingend über den Automaten hergestellt werden, sondern kann, ebenso wie die genannten Zusatzfunktionen gänzlich über die Netzwerkverbindung des Kunden und auch über sein Gerät mit der entsprechenden Applikation abgewickelt werden.

[0006] Aus dem Flussdiagramm in **Fig. 1** ist unmittelbar ersichtlich, wie der Automat, obwohl er nicht an das Netzwerk angebunden ist, dennoch Tokens oder Coins an die Kunden verkaufen kann und die Wallet, von der aus die Coins oder Tokens verkauft werden, immer nur das erforderliche Mindestguthaben aufweist, dieses aber sicher und ohne Engpass ausliefern kann.

technische Ausführung

[0007] In dieser Darstellung wird auf die nähere Erklärung von Ausführungsschritten und -details, die ein Fachmann ohne besondere Erklärung umsetzen kann, verzichtet.

[0008] Das System besteht aus dem eigentlichen Automaten, der für Benutzer zugänglich ist und einem Überwachungssystem, das an einem beliebigen Ort mit Anbindung an das Netzwerk untergebracht sein kann. Der Benutzer benötigt ein Gerät, das in der Lage ist, eine Transaktion an das Netzwerk zu übermitteln, beispielsweise ein Smartphone mit einer App zum Verwalten von kryptographischen Coins oder Tokens. Dieses Gerät und die App muss der Kunde nicht notwendigerweise selbst bereitstellen; sie können auch eine Erweiterung des Automaten sein, so dass außer einer Identifizierung des Kunden, die die Wallet entsperrt und den Zugriff auf den privaten Schlüssel freigibt, vom Kunden keine weite-

re Aktion verlangt wird. Die Identifizierung kann leicht anhand biometrischer Merkmale o.a. vorgenommen werden.

[0009] Der Automat besteht in seiner Mindestkonfiguration aus einem Modul zum Annehmen der Bezahlung, falls die Tokens gegen Bezahlung ausgegeben werden sollen, einer Vorrichtung zum Eingeben der Walletadresse, an die der Benutzer das Guthaben transferiert haben möchte, einer Computereinheit mit RAM-Speicher, einem Ausgabegerät für die Transaktionssignatur und den konstruktiv notwendigen Teilen wie Chassis, Energieversorgung, Verbindungskabel usw.

[0010] Das zum Betrieb zusätzlich erforderliche Überwachungssystem dient zur laufenden Feststellung des noch auf der Walletadresse des Automaten vorhandenen Guthabens und dem Auffüllen desselben bei Bedarf. Das Überwachungssystem wird vom Betreiber oder einem beauftragten Dienstleister betreut. Es besteht aus einem an das Netzwerk angeschlossenen Computer mit einer Software, die regelmäßig die Blockchain oder eine andere verteilte oder eine zentrale Datenbank abfragt und das Guthaben durch das Initiieren von Transaktionen zugunsten der Walletadresse auf dem erforderlichen Stand hält, so dass der Automat nie „leer“ wird. Eine entsprechende Software zu produzieren, ist jedem durchschnittlichen Programmierer möglich und somit trivial. Im Speicher des Automaten kann das Logfile mit allen gewünschten Daten über die Nutzung des Automaten zur späteren Auswertung aufgezeichnet werden; bei Systemen, die über eine Netzwerkanbindung verfügen, lassen sich die Daten in Echtzeit an ein entferntes System übertragen.

[0011] Da der Automat die Transaktionen signiert, ist es erforderlich, dass der Automat auf den privaten Schlüssel seiner Wallet zugreifen kann. Das Guthaben auf der Adresse kann zwar dadurch, dass das Guthaben aus der Ferne beliebig und laufend erhöht werden kann, immer auf dem niedrigsten, erforderlichen Stand gehalten werden, so dass ein Unbefugter, der den Automaten gewaltsam öffnet, um aus dem Speicher den Schlüssel auszulesen, nur geringe Werte erbeuten kann. Aber auch gegen diesen Verlust kann ein Schutz aufgestellt werden, indem der Schlüssel räumlich entfernt gespeichert wird, wofür schon ein Nebenraum ausreichend sein kann, und eine kabelgebundene oder andere Verbindung dem Automaten das Verwenden des Schlüssels erlaubt. Um den privaten Schlüssel völlig sicher vor dem Zugriff von Unbefugten unterzubringen, kann die gesamte Software oder ein Teil davon in einem virtuellen Laufwerk untergebracht werden, das sich in einem sicher verschlüsselten Container, zum Beispiel in einem Truecrypt-Container oder einem anderen geeigneten, verschlüsselten, logischen Container befindet. Das Brechen der Verschlüsselung würde mehr Ressourcen verbrauchen als an Gewinn durch den Diebstahl zu realisieren ist, wodurch ein Einbruchsversuch sinnlos wird. Die Rechnerhardware oder auch nur deren physische Steckerplätze sind so mit einem Stromunterbrecher verbunden, dass beim Öffnen des Chassis oder dem Versuch, an die Buchsen zu gelangen, die Stromzufuhr unterbrochen wird, das System abstürzt und der Container ohne sein Passwort nicht mehr geöffnet werden kann und somit der private Schlüssel und andere sensible Informationen für den Angreifer unerreichbar sind. In der banalsten Ausführung reicht es aus, den gesamten Automaten so an eine rückwärtige Zimmerwand zu stellen, dass ein handelsüblicher Tastschalter, wie er für Stehlampen verwendet wird, durch das Eigengewicht des Automaten gedrückt gehalten wird. Sobald der Taster losgelassen wird, also beim Abrücken des Gerätes von der Wand, schaltet er ab, und aus dem nun stromlosen Automaten können keinerlei Daten mehr ausgelesen werden selbst nachdem die Energiezufuhr wiederhergestellt wird, sofern das Containerpasswort nicht bekannt ist.

[0012] Selbstverständlich lässt sich das Prinzip auch in umgekehrter Weise anwenden, so dass der Automat es ist, der die Coins oder Tokens von einem Kunden annimmt, dessen App die Transaktion signiert, ohne dass dieser Netzanbindung benötigt. Entsprechend würde der Automat dann keine Zahlungsmittel annehmen, sondern Ware ausgeben. In dieser Umkehrung entsteht so ein Warenverkaufsautomat. Wenn der Kunde dabei keine werthaltigen Coins oder Tokens zum Transfer freigibt, sondern solche die als unverfälschbarer Identitätsnachweis oder fälschungssicherer Zugangsausweis dienen und anstatt dass Waren ausgegeben werden, eine Durchgangssperre geöffnet wird, dient der Automat als manipulationsresistentes Zugangs- und Personenkontrollsystem. Wenn keine begrenzte Anzahl von individuellen Einlassvorgängen angestrebt wird, kann von der zu kontrollierenden Person zur Vereinfachung auch das Signieren eines sogenannten Datachunks (Bezugsdatenblock) verlangt werden, was in Kombination mit den anderen hier beschriebenen Varianten insbesondere für den Verkauf von Waren, die mit einer Identitätsfeststellung des Käufers einhergehen sollen, von Nutzen ist. In Unternehmen oder Regimen, die zum Kontrollieren ihrer Mitarbeiter oder Untertanen oder aus Gründen der tatsächlichen oder vorgeblichen Terrorabwehr oder mit anderen Absichten Telefonkarten, Computer und andere Geräte mit personenbezogenen Daten des Besitzers verknüpfen wollen, gibt es dafür ebenso Verwendung wie in der militärischen Anwendung.

[0013] In einer weiteren Variante nimmt der Automat weder Geld an, noch gibt er Ware aus, sondern sowohl Kunde als auch Automat signieren jeweils nur kryptographische Transaktionen und geben sich gegenseitig die Signaturen bekannt, wodurch ein Ge-

rät entsteht, das ohne blockchainimmanente Smart Contracts kryptograhische Coins oder Tokens gegeneinander wechseln kann und somit blockchainanalyseresistent ist.

[0014] Die Varianten können beliebig kombiniert werden, wodurch sich ein weites Feld von Anwendungsmöglichkeiten eröffnet.

[0015] Sofern die öffentliche Adresse des Kunden ohne sein besonderes Zutun ermittelt werden kann, ist es nicht einmal erforderlich, dass der Kunde seine öffentliche Adresse für jeden Transfer erneut zum Zweck des Auslesens übermittelt. Es gibt viele Möglichkeiten, den Kunden zu identifizieren. Dazu gehören das Abgleichen von gespeicherten Verhaltens- und Bewegungsmustern oder das Erfassen von biometrischen Merkmalen. Gängige Verfahren sind die Auswertung der zeitlichen Abstände zwischen Tastaturanschlägen oder das Vorlesenlassen eines Datachunks, um durch Auswertung der Stimmencharakteristika und der Mikropausen zwischen den Wörtern die Identität festzustellen. Solche Verfahren sind in Abhängigkeit von der herrschenden Rechtslage oft mit einer geringeren Beeinträchtigung des Nutzungserlebnisses verbunden als ein Irisscan o. ä., für die meist - lästig aus Sicht des Kunden - eine separate Einwilligung vom Kunden eingeholt werden muss. Wenn der Kunde vom System erkannt worden ist, kann seine öffentliche Adresse leicht aus einer Datenbank ermittelt werden.

[0016] So lassen sich in Verbindung mit dem Vorhergenannten auf dann triviale Weise Automaten herstellen, die sich als Teilnehmer am Internet of Things gegenseitig versorgen und untereinander abrechnen - der Kunde bei einem Automaten kann selbst ein Automat oder Roboter sein - und das Guthaben des Kunden zeit- und verbrauchskongruent, fehlerfrei belasten. Der Kunde braucht dann nur noch seinen Wunsch zu äußern, zum Beispiel welches Getränk er aus dem Automaten ziehen will oder welche Summe an Kryptotokens er gegen Belastung seines herkömmlichen oder auf kryptographischer Basis geführten Kundenkontos erwerben will, und der Automat erfüllt diesen Wunsch, ohne dass der Kunde die Bezahlung oder Abrechnung durch irgendeine Handlung bestätigen oder initiieren muss.

[0017] Eine Variante, die vollständig auf jegliche Aktion des Kunden verzichtet, würde ein Zusatzmodul enthalten, das die vom Automaten oder dem Gerät des Kunden signierte Transaktion automatisiert an das Netzwerk sendet. Weiterhin ist es nach heutigem Stand der Technik trivial, aus der Auswertung der Handlungen und Verhaltensmuster des Kunden mit großer Treffergenauigkeit vorzusagen, welche Wünsche und Impulse in den kommenden Minuten in das Bewusstsein des Kunden gelangen werden. Somit muss der Kunde noch nicht einmal seine Wünsche äußern. In einem Anwendungsbeispiel könnte es so aussehen, dass der Kunde ein Restaurant betritt - wobei das Netzwerk bereits heute ohne Mühe vorhersagen kann, wann und welches Restaurant der Kunde nach seinem Verständnis „spontan“ wählt - und der Automat den Kunden erkennt, berechnet, was der Kunde konsumieren möchte, prüft, ob sein Vermögen ausreichend ist, um die Rechnung zu begleichen und dann - wenn der Kunde die erforderliche Bonität hat und ihm Einlass gewährt wurde - ohne dass der Kunde sich äußern muss, das Gewünschte serviert. Der Kunde kann jederzeit ohne durch einen Bezahlvorgang aufgehalten zu werden, das Lokal verlassen, und die Rechnung wird dennoch bezahlt. Solche Automaten können für den Kunden unsichtbar in jedes bestehende Verkaufs- oder Warenverteil- und Dienstleistungssystem eingebaut oder sogar vollständig virtualisiert betrieben werden.

[0018] In letzter Konsequenz ergibt sich daraus eine vollautomatisierte und maschinengestützte, arbeitsfreie und ökonomisch gerechte Gesellschaft.

ZITATE ENTHALTEN IN DER BESCHREIBUNG

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

Zitierte Patentliteratur

- US 9135787 B1 [0003]
- KR 1020160074178 A [0003]

Patentansprüche

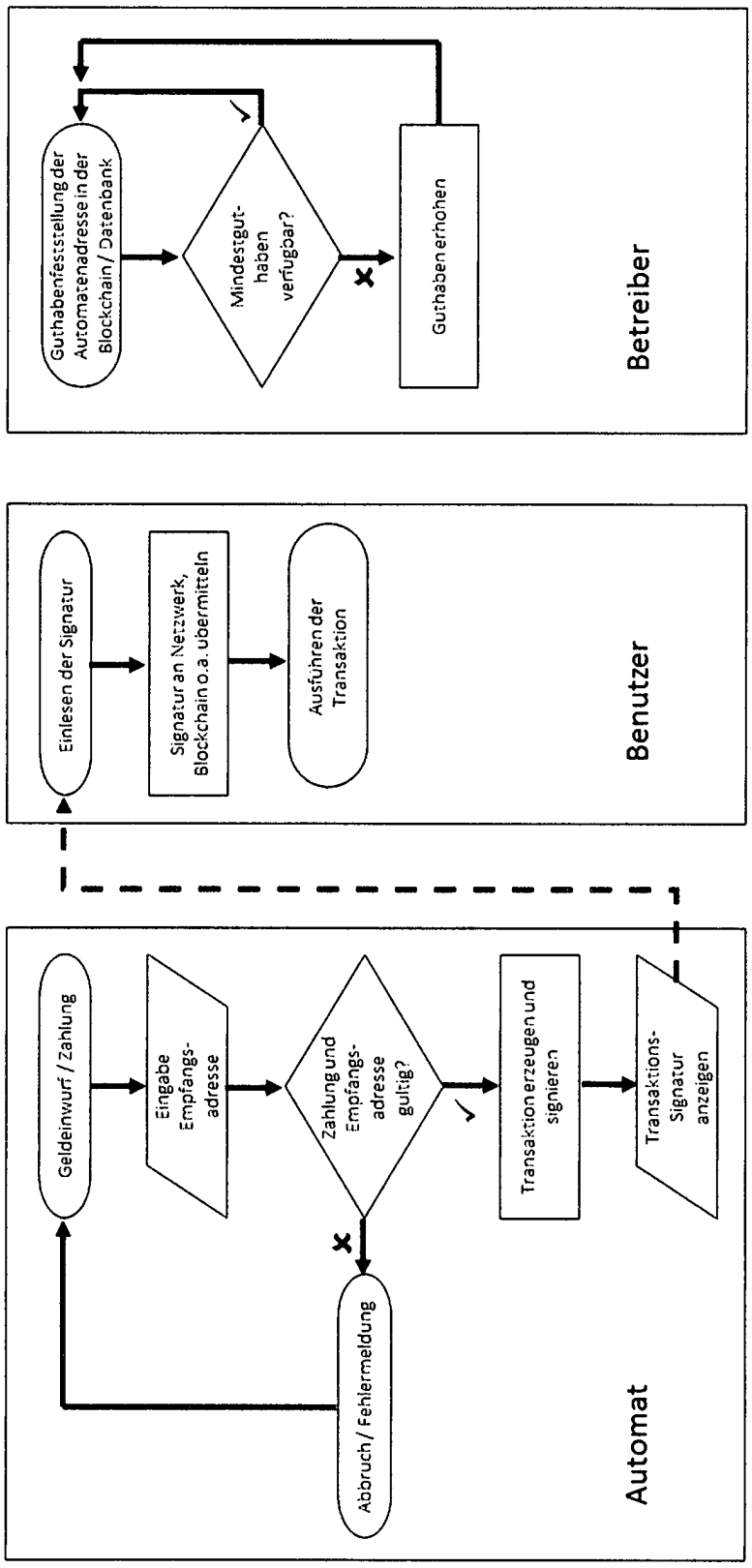
1. Automat zur Übertragung, respektive Ausgabe, von virtuellen oder elektronischen Zahlungsmitteln und/oder kryptographischen Währungseinheiten und Gutscheinen, gekennzeichnet dadurch, dass der Automat nicht mit einem Netzwerk verbunden ist und auch keine vorgefertigten Wallets oder Transaktionen gespeichert hat, sondern an den Benutzer die vom Automaten erzeugte Transaktionssignatur ausgibt, die der Automat auf Anforderung durch den Benutzer so erzeugt, dass diese Transaktionssignatur geeignet ist, einen Guthabentransfer auf die Adresse auszulösen, die der Automat als dem Benutzer zugehörig ermittelt hat, ohne dass der Automat die Signatur selbst an das Netzwerk übermittelt und gekennzeichnet dadurch, dass der Speicherort des privaten Schlüssels des Automaten für den Benutzer und andere Unbefugte durch konstruktive und/oder logische Hindernisse unzugänglich ist und weiters **dadurch gekennzeichnet**, dass das Guthaben der dem Automaten zugehörigen Adresse in Echtzeit über die Abfrage der Blockchain oder einer anderen verteilten oder zentralen oder anderen Datenbank vom Betreiber des Automaten ermittelt wird und das Guthaben von einem beliebigen Ort aus durch Transaktion zu Gunsten der Adresse des Automaten aufgefüllt werden kann.

2. Automat, nach dem in Schutzanspruch 1 beschriebenen Prinzip, gekennzeichnet dadurch, dass die Rollen von Automat und Benutzer in der Weise vertauscht sind, dass nicht der Automat im Gegenzug dafür, dass der Benutzer Geld an den Automaten gibt, vom Automaten kryptographische Coins oder Tokens erhält, sondern der Benutzer die Coins oder Tokens an den Automaten gibt und der Automat eine Ware ausgibt oder eine Dienstleistung veranlasst oder kryptographische Coins oder Tokens oder eine Transaktionssignatur ausgibt.

3. Automat, gekennzeichnet dadurch, dass er die Eigenschaften und Funktionen aufweist, wie sie sowohl in den Schutzansprüchen 1 als auch 2 beschrieben sind.

Es folgt eine Seite Zeichnungen

Anhängende Zeichnungen



Figur 1