(19) SCHWEIZERISCHE EIDGENOSSENSCHAFT
EIDGENÖSSISCHES INSTITUT FÜR GEISTIGES EIGENTUM

(11) **CH 717 898 B1**

(51) Int. Cl.: ***G06Q 40/06*** *(2012.01)*
G06Q 20/02 *(2012.01)*
H04L 9/32 *(2006.01)*

Erfindungspatent für die Schweiz und Liechtenstein
Schweizerisch-liechtensteinischer Patentschutzvertrag vom 22. Dezember 1978

(12) PATENTSCHRIFT

(21) Anmeldenummer: 001213/2020

(22) Anmeldedatum: 24.09.2020

(43) Anmeldung veröffentlicht: 31.03.2022

(24) Patent erteilt: 13.09.2024

(45) Patentschrift veröffentlicht: 13.09.2024

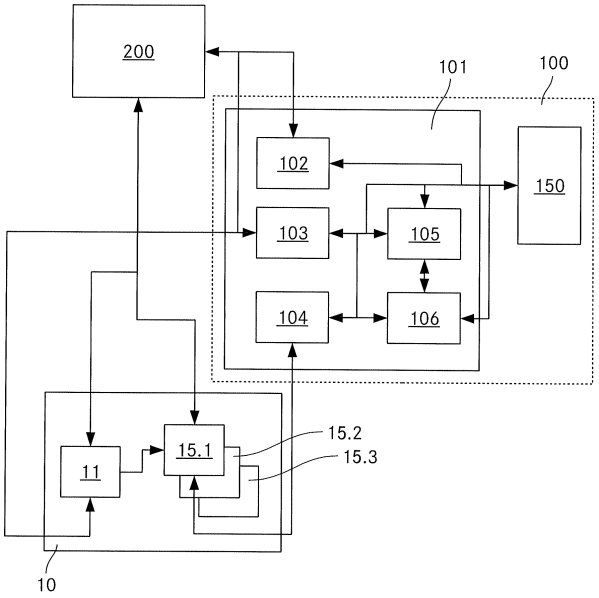
(73) Inhaber:
Obligate AG, Stadthausquai 15
8004 Zürich (CH)

(72) Erfinder:
Daniel Killenberger, 4054 Basel (CH)
Elliot Walmsley, CT9 1NY, Kent (GB)
Samuel Emde, 4056 Basel (CH)
Stephan D. Meyer, 8570 Weinfelden (CH)
Thomas Bocek, 8050 Zürich (CH)

(74) Vertreter:
Keller Schneider Patent- und Markenanwälte AG (Bern),
Eigerstrasse 2 Postfach
3000 Bern 14 (CH)

(54) Server zur Abwicklung von Finanz-Transaktionen.

(57) Ein Server (101) zur Abwicklung von Transaktionen ist zur Verbindung mit einem Computernetzwerk ausgebildet, das einen Distributed Ledger (150) speichert, welcher eine Mehrzahl von Datenblöcken umfasst, die zwischen mehreren Rechnern des Computernetzwerks repliziert, geteilt und synchronisiert sind. Der Server (101) umfasst ein Verknüpfungsmodul (102), das eingerichtet ist zum Empfangen eines öffentlichen Schlüssels einer Zertifizierungsstelle (200) und zum Generieren und Speichern von Fingerprintdaten, die den öffentlichen Schlüssel repräsentieren, in einem der Datenblöcke des Distributed Ledger (150). Der Server (101) umfasst weiter ein Berechtigungsmodul (103), das eingerichtet ist zum Speichern von Zugriffsberechtigungen, die mit von der Zertifizierungsstelle (200) ausgegebenen Identitätszertifikaten verknüpft sind, in einem der Datenblöcke des Distributed Ledger (150). Er umfasst weiter ein Eingangsmodul (104), das eingerichtet ist zum Empfangen einer Transaktionsanforderung von einer anfordernden Stelle (10), wobei die Anforderung mit dem privaten Schlüssel der anfordernden Stelle (10) signiert ist, der mit einem öffentlichen Schlüssel eines von der Zertifizierungsstelle (200) ausgegebenen Identitätszertifikats der anfordernden Stelle (10) verknüpft ist. Der Server (10) umfasst weiter ein Überprüfungsmodul (105), das eingerichtet ist zum Überprüfen einer Identität der anfordernden Stelle (10), gestützt auf die Anforderung der anfordernden Stelle (10), den gespeicherten Fingerprintdaten und den gespeicherten Zugriffsberechtigungen, und ein Aufzeichnungsmodul (106), das eingerichtet ist zum Aufzeichnen einer Transaktion, die der Transaktionsanforderung entspricht, in einem Datenblock des Distributed Ledger (150), sofern die Identität erfolgreich durch das Überprüfungsmodul (105) verifiziert wurde.



Beschreibung

Technisches Gebiet

[0001] Die Erfindung betrifft einen Server zur Abwicklung von Transaktionen, wobei der Server zur Verbindung mit einem Computernetzwerk ausgebildet ist, das einen Distributed Ledger speichert, welcher eine Mehrzahl von Datenblöcken umfasst, die zwischen mehreren Rechnern des Computernetzwerks repliziert, geteilt und synchronisiert sind. Die Erfindung betrifft weiter ein entsprechendes computergestütztes System und ein Verfahren zur Abwicklung von Transaktionen.

Stand der Technik

[0002] Herkömmlich wurden Transaktionen mit Wertpapieren, z. B. solche in Bezug auf Wechsel, gestützt auf physische Dokumente, abgewickelt. Dies ist aber gerade im internationalen Verkehr oder bei kurzfristigen Geschäften sehr umständlich. Es besteht entsprechend ein Bedürfnis, solche Transaktionen rein elektronisch durchzuführen. Dabei sind strenge finanzrechtliche Vorschriften zu beachten - zudem kommt es bei solchen Transaktionen oft entscheidend darauf an, dass sich die beteiligten Parteien einander gegenüber verlässlich identifizieren.

[0003] Es sind zahlreiche Verfahren zur elektronischen Abwicklung von Finanztransaktionen bekannt. Sie lassen sich üblicherweise in zwei Gruppen unterteilen: Verfahren der ersten Gruppe bedienen sich eines Dienstleisters (Trusted Third Party), der von allen beteiligten Parteien als vertrauenswürdig eingestuft wird und die Transaktion im Auftrag der Parteien abwickelt. Verfahren der zweiten Gruppe basieren auf der so genannten Distributed-Ledger-Technologie (DLT), bei der die Daten in einem Computernetzwerk abgelegt sind, und zwar in einer Mehrzahl von Datenblöcken, die zwischen mehreren Rechnern des Computernetzwerks repliziert, geteilt und synchronisiert sind. Die Datenblöcke sind untereinander so verknüpft, dass neue Transaktionen innerhalb des Netzwerks stets nachgeführt werden und bei divergierenden Dateninhalten Konsens geschaffen wird, welche Daten als korrekt anzusehen sind. Sicherheit wird zudem durch den Einsatz von kryptografischen Verfahren und elektronischen Signaturen geschaffen. Ein Beispiel einer DLT bildet die Blockchain-Technologie.

[0004] DLT-Anwendungen haben in der Regel u. a. zum Ziel, dass sich der Einsatz einer TTP erübrigt. Zur Abwicklung anonymer Transaktionen sind DLT-Anwendungen denn auch sehr gut geeignet. Anforderungen zur Identifizierung kann in deren Rahmen aber oft nicht auf einfache Weise Genüge getan werden.

Darstellung der Erfindung

[0005] Aufgabe der Erfindung ist es, einen dem eingangs genannten technischen Gebiet zugehörenden Server zu schaffen, der eine effiziente Abwicklung von Transaktionen bei sicherer Identifikation der Transaktionspartner ermöglicht.

[0006] Die Lösung der Aufgabe ist durch die Merkmale des Anspruchs 1 definiert. Gemäss der Erfindung umfasst der Server zur Abwicklung von Transaktionen folgendes:

a) ein Verknüpfungsmodul, das eingerichtet ist zum Empfangen eines öffentlichen Schlüssels einer Zertifizierungsstelle und zum Generieren und Speichern von Fingerprintdaten, die den öffentlichen Schlüssel repräsentieren, in einem der Datenblöcke des Distributed Ledger;

b) ein Berechtigungsmodul, das eingerichtet ist zum Speichern von Zugriffsberechtigungen, die mit von der Zertifizierungsstelle ausgegebenen Identitätszertifikaten verknüpft sind, in einem der Datenblöcke des Distributed Ledger;

c) ein Eingangsmodul, das eingerichtet ist zum Empfangen einer Transaktionsanforderung von einer anfordernden Stelle, wobei die Anforderung mit dem privaten Schlüssel der anfordernden Stelle signiert ist, der mit einem öffentlichen Schlüssel eines von der Zertifizierungsstelle ausgegebenen Identitätszertifikats der anfordernden Stelle verknüpft ist;

d) ein Überprüfungsmodul, das eingerichtet ist zum Überprüfen einer Identität der anfordernden Stelle, gestützt auf die Anforderung der anfordernden Stelle, den gespeicherten Fingerprintdaten und den gespeicherten Zugriffsberechtigungen;

e) ein Aufzeichnungsmodul, das eingerichtet ist zum Aufzeichnen einer Transaktion, die der Transaktionsanforderung entspricht, in einem Datenblock des Distributed Ledger, sofern die Identität erfolgreich durch das Überprüfungsmodul verifiziert wurde.

[0007] Ein erfindungsgemässes computergestütztes System für die Abwicklung von Transaktionen umfasst entsprechend:

a) eine Zertifizierungsstelle zur Ausgabe von Identitätszertifikaten, wobei die Identitätszertifikate einen öffentlichen Schlüssel und eine Identität umfassen und von der Zertifizierungsstelle signiert sind;

b) ein Computernetzwerk, das einen Distributed Ledger speichert, welcher eine Mehrzahl von Datenblöcken umfasst, die zwischen mehreren Rechnern des Computernetzwerks repliziert, geteilt und synchronisiert sind;

c) einen erfindungsgemässen Server zur Abwicklung von Transaktionen wie vorstehend beschrieben.

[0008] Ein erfindungsgemässes Verfahren zur Abwicklung von Transaktionen, umfasst zudem entsprechend die folgenden Schritte:

a) Speichern von Fingerprintdaten, die den öffentlichen Schlüssel einer Zertifizierungsstelle repräsentieren, in einem einer Mehrzahl von Datenblöcken eines Distributed Ledger, wobei die Mehrzahl von Datenblöcken zwischen mehreren Rechnern eines Computernetzwerks repliziert, geteilt und synchronisiert sind;

b) Speichern von Zugriffsberechtigungen, die mit von der Zertifizierungsstelle ausgegebenen Identitätszertifikaten verknüpft sind, in einem der Mehrzahl von Datenblöcken des Distributed Ledger;

c) Empfangen einer Transal<tionsanforderung einer anfordernden Stelle, wobei die Anforderung mit dem privaten Schlüssel der anfordernden Stelle signiert ist, der mit einem öffentlichen Schlüssel eines von der Zertifizierungsstelle ausgegebenen Identitätszertifikats der anfordernden Stelle verknüpft ist;

d) Überprüfung einer Identität der anfordernden Stelle, gestützt auf die Anfrage der anfordernden Stelle, den gespeicherten Fingerprintdaten und den gespeicherten Zugriffsberechtigungen;

e) Aufzeichnen einer Transaktion, die der Transaktionsanforderung entspricht, in einem Datenblock des Distributed Ledger, sofern die Identität erfolgreich durch das Überprüfungsmodul verifiziert wurde.

[0009] „Server“ ist im Rahmen der vorliegenden Anmeldung breit zu verstehen. Es handelt sich um Rechnermittel, die Daten empfangen, verarbeiten und ausgeben können. Ein Server im Sinn der vorliegenden Anmeldung kann durch einen einzelnen Rechner oder mehrere Rechner gebildet und ganz oder teilweise virtualisiert sein.

[0010] Beim Distributed Ledger handelt es sich insbesondere um eine private Blockchain. Die Zertifizierungsstelle ist ein vertrauenswürdiger Dritter (Trusted Third Party, TTP).

[0011] Bei den Fingerprintdaten kann es sich um den öffentlichen Schlüssel selbst handeln oder um ein Verarbeitungsergebnis (digest), das aus dem öffentlichen Schlüssel bzw. dem Zertifikat gewonnen wird. Entsprechend können die Fingerprintdaten nebst dem öffentlichen Schlüssel weitere Informationen umfassen bzw. aus weiteren Informationen gewonnen werden.

[0012] Die Identitätszertifikate werden insbesondere gestützt auf den Standard X.509 erzeugt. Die Verknüpfung der Zugriffsberechtigungen mit den Identitätszertifikaten erfolgt insbesondere anhand einer eindeutigen Kennung (serial number) der jeweiligen Zertifikate. Die Verknüpfung der Transaktionsanforderungen mit einem öffentlichen Schlüssel eines Identitätszertifikats erfolgt insbesondere durch die Anwendung einer qualifizierten elektronischen Signatur (OES). Entsprechende Zertifikate umfassen jeweils mindestens zwei miteinander verkettete Zertifikate, namentlich das Nutzerzertifikat und eines oder mehrere Herausgeberzertifikate. Mithilfe der entsprechenden Zertifikatskette kann verifiziert werden, dass das QES-Identitätszertifikat vom entsprechenden Herausgeber, namentlich der entsprechenden Zertifizierungsstelle (TTP), stammt.

[0013] Die Transaktionsanforderung wird unabhängig vom Distributed Ledger („off-chain“) von der anfordernden Stelle (oder im Auftrag der anfordernden Stelle) erzeugt und umfasst bereits die zur Überprüfung der Identität der anfordernden Stelle notwendigen Informationen. Die Überprüfung selbst erfolgt dann anhand von Daten, die im Distributed Ledger abgelegt sind („on-chain“).

[0014] Die Aufzeichnung der Transaktion kann von weiteren Bedingungen abhängig sein, z. B. in Bezug auf die Möglichkeit oder Gültigkeit der Transaktion selbst.

[0015] Der erfindungsgemässe Server und das erfindungsgemässe Verfahren zeichnen sich dadurch aus, dass Zertifikate, die von TTP ausgestellt werden, mit Distributed-Ledger-Technologie (DLT) verknüpft werden. Transaktionsdaten lassen sich somit zuverlässig und sicher in einem Distributed Ledger ablegen, was z. B. auch die Nutzung von Smart Contracts ermöglicht. Gleichzeitig kann Anforderungen Genüge getan werden, die eine Identifizierung der involvierten Parteien verlangen. Solche Anforderungen ergeben sich z. B. aus rechtlichen Bestimmungen zur Regulierung von Finanztransaktionen, die Identifizierbarkeit kann aber natürlich auch von den beteiligten Parteien selbst gewünscht sein.

[0016] Die DLT (zur Abwicklung der eigentlichen Transaktionen) wird also mit der Nutzung einer TTP oder mehrerer TTPs (zur Sicherstellung der Identifikation) in einer neuartigen Weise verknüpft, um die Vorteile beider Ansätze miteinander zu verbinden.

[0017] Die Transaktionsanfrage kann insbesondere die Ausgabe, die Übertragung oder die Verrechnung von Finanzinstrumenten, insbesondere von Wechseln (promissory notes), betreffen. Das erfindungsgemässe System dient somit zur

Verwaltung von digitalen Sicherheitszertifikaten (digital security certificates). In diesem Zusammenhang ist es für die beteiligten Parteien essenziell, Sicherheit über die Identität der Transaktionspartner zu haben. Eine Identifizierung ist auch aufgrund regulatorischer Anforderungen oft zwingend.

[0018] Die Erfindung lässt sich auch im Zusammenhang mit anderen Transaktionen, z. B. im Finanz- und Immobilienbereich, einsetzen, insbesondere dort, wo eine sichere Identifikation von den Parteien und/oder aufgrund rechtlicher Vorschriften gefordert ist.

[0019] Mit Vorteil ist das Berechtigungsmodul eingerichtet zum Speichern von Zuordnungen zu Identitätszertifikaten von Administratoren, das Eingangsmodul ist eingerichtet zum Empfangen von Transaktionsanforderungen, die ein Zugriffszertifikat mit einer Signatur eines Administrators umfassen, und das Überprüfungsmodul ist eingerichtet zur Prüfung, ob die Signatur des Administrators mit einem der Identitätszertifikate der gespeicherten Zugriffsberechtigungen verknüpft ist.

[0020] Somit sind im Rahmen des erfindungsgemässen Verfahrens den Zugriffsberechtigungen Identitätszertifikate von Administratoren zugeordnet, die Transaktionsanforderung der anfordernden Stelle umfasst ein Zugriffszertifikat mit einer Signatur eines Administrators, und eine erfolgreiche Überprüfung der Identität setzt voraus, dass die Signatur des Administrators mit einem der Identitätszertifikate der gespeicherten Zugriffsberechtigungen verknüpft ist.

[0021] Die Zuordnung zu den Identitätszertifikaten erfolgt insbesondere mit Hilfe einer eindeutigen Kennung (serial number) der Zertifikate. Daneben ist mit Vorteil der Herausgeber (Zertifizierungsstelle) vermerkt, so dass bei Bedarf Identitätszertifikate verschiedener Herausgeber ohne Weiteres genutzt werden können, vorausgesetzt entsprechende Fingerprintdaten dieser Herausgeber sind wie oben erläutert im Distributed Ledger abgelegt.

[0022] Administratoren können nun - gestützt auf deren Identitätszertifikate - weiteren Personen die Berechtigung zur Anforderung von Transaktionen erteilen, indem sie diesen ein Zugriffszertifikat zur Verfügung stellen. Dabei handelt es sich im Wesentlichen um eine Datenportion, die vom Administrator signiert ist, insbesondere mit einer QES. Die Erteilung solcher Berechtigungen erfolgt auf diese Weise ausserhalb des Distributed Ledger (off-chain). Die Prüfung der Berechtigung erfolgt anhand der on-chain gespeicherten Zugriffsberechtigung des Administrators, des Zugriffszertifikats, also der Datenportion mit der Signatur des Administrators, und des Identitätszertifikats der anfordernden Stelle.

[0023] Daneben werden natürlich alle involvierten Identitätszertifikate auf ihre Gültigkeit hin geprüft, wie oben erläutert wiederum mit Hilfe von Daten, die on-chain gespeichert sind (Fingerprintdaten).

[0024] Bevorzugt umfasst das Zugriffszertifikat eine eindeutige Kennung der anfordernden Stelle (z. B. eine eindeutige Kennung des Identitätszertifikats) und eine Zuordnung zu einer Entität. Dadurch wird sichergestellt, dass das Zugriffszertifikat nur von einer designierten, eindeutig identifizierten Person, zur Anforderung von Transaktionen genutzt werden kann, sie also nicht an andere Personen übertragbar ist. Zudem lassen sich jeweils mehrere Administratoren und/oder berechtigte anfordernde Stellen einer gemeinsamen Entität zuordnen. Bei den Administratoren und berechtigen Stellen handelt es sich insbesondere um natürliche Personen (für welche gängigerweise Identitätszertifikate ausgegeben werden können), bei der Entität handelt es sich insbesondere um eine juristische Person, z. B. ein Unternehmen. Die Zuordnung zur Entität erfolgt beispielsweise über standardisierte, staatlich verwaltete Nummern (z. B. Unternehmensnummern bzw. - Kennziffern, ergänzt mit einer Angabe zur jeweiligen Jurisdiktion).

[0025] Im Rahmen der Erfindung können somit auch grosse und komplex organisierte Unternehmen auf einfache Weise abgebildet werden, indem im Distributed Ledger letztlich nur die Administratoren verwaltet werden müssen, während die Verwaltung der spezifischen Berechtigungen unternehmensintern durch das Ausstellen der Zugriffszertifikate erfolgt.

[0026] Die Datenportion des Zugriffszertifikats kann weitere Informationen umfassen, z. B. in Bezug auf die Zeichnungsrechte (signing rights) der berechtigten Person. So kann z. B. vermerkt sein, dass die Person nur zusammen mit einer weiteren (spezifizierten oder nicht spezifizierten) berechtigten Person der Entität gemeinsam wirksam signieren kann.

[0027] Die Zugriffszertifikate haben mit Vorteil eine beschränkte zeitliche Gültigkeit, so dass Berechtigungen regelmässig überprüft werden müssen.

[0028] In einer einfacheren, alternativen Ausführungsform der Erfindung werden direkt die Zugriffsberechtigungen der berechtigten Nutzer on-chain gespeichert. Es ist auch möglich, beide Varianten in demselben System zu ermöglichen, d. h. es können sowohl direkt berechtigte als auch delegiert, berechtigte Stellen Transaktionsanforderungen stellen.

[0029] Mit Vorteil umfasst die Überprüfung der Identität der anfordernden Stelle eine Überprüfung, ob die anfordernde Stelle nicht in einer Widerrufsliste aufgeführt ist, die in einem Datenblock des Distributed Ledgers gespeichert ist.

[0030] Dadurch kann sichergestellt werden, dass nicht mehr berechtigte Stellen keine gültigen Transaktionsanforderungen mehr stellen können, denn Nutzer mit gültigem Identitätszertifikat können weiterhin Daten qualifiziert elektronisch signieren und on-chain ist nicht bekannt, welche Stellen von den verzeichneten Administratoren durch Ausstellung entsprechender Zugriffszertifikate berechtigt wurden.

[0031] Bevorzugt sind die folgenden Elemente on-chain gespeichert:

– die Transaktionsdaten (ggf. einschliesslich der Finanzinstrumente in virtueller Form);

- Daten zur Identifikation der Echtheit der Zertifikate zugelassener Zertifikationsdienste;
- die berechtigten Administratoren mit Zuordnung zur jeweiligen juristischen Person;
- die Widerrufsliste.

[0032] Die Zugriffszertifikate sind dagegen mit Vorteil off-chain gespeichert, indem diese mittels Zertifikaten von den Administratoren erteilt und bei Transaktionen jeweils im Rahmen der Transaktionsanforderung übermittelt werden. Auch die Erteilung der Identitätszertifikate erfolgt off-chain, insbesondere durch eine vom System unabhängige Zertifizierungsstelle.

[0033] Die Transaktion kann vor der Aufzeichnung unter Verwendung einer symmetrischen Verschlüsselung verschlüsselt werden, so dass Transaktionen durch Löschen eines Ver-/Entschlüsselungsschlüssels verworfen werden können.

[0034] Nach Erhalt und erfolgreicher Prüfung einer Transaktionsaufforderung wird der Inhalt der Transaktion somit mit Hilfe des symmetrischen Verschlüsselungsverfahrens (z. B. AES 256 bit) verschlüsselt und im Distributed Ledger abgelegt. Wenn der Ver-/Entschlüsselungsschlüssel gelöscht wird, kann auf die entsprechende Information nicht mehr zugegriffen werden. Die Transaktion ist somit nicht mehr ersichtlich und so auch nicht mehr wirksam.

[0035] Mit Vorteil können Transaktionsanforderungen von mehreren (zwei oder mehr) Parteien unterzeichnet werden. Eine entsprechende Transaktionsanforderung ist also von zusätzlichen Parteien unterzeichnet, die an der aufzuzeichnenden Transaktion beteiligt sind, und die Identität der zusätzlichen Parteien wird auf der Grundlage der jeweiligen gespeicherten Fingerprintdaten und gespeicherten Zugriffsberechtigungen überprüft.

[0036] Solche Transaktionen beinhalten beispielsweise die Übertragung oder Begleichung eines Wechsels, wo der alte und der neue Inhaber bzw. der Herausgeber und der (aktuelle) Inhaber unterzeichnen müssen, damit die Transaktion gültig ist.

[0037] In Anwendungen, wo die Identität der beteiligten Parteien durch einen gesonderten Prozess überprüft werden muss, z. B. im Rahmen von „Know Your Customer"-Anforderungen im Finanzbereich, kann das Speichern der Zugriffsberechtigungen in einem Datenblock zusätzlich von einer Identitätsprüfung abhängig gemacht werden, die unabhängig ist vom Identitätszertifikat.

[0038] Eine solche Prüfung beinhaltet beispielsweise ein reales oder virtuelles Interview, die Prüfung von Ausweisdokumenten usw.

[0039] Aus der nachfolgenden Detailbeschreibung und der Gesamtheit der Patentansprüche ergeben sich weitere vorteilhafte Ausführungsformen und Merkmalskombinationen der Erfindung.

Kurze Beschreibung der Zeichnungen

[0040] Die zur Erläuterung des Ausführungsbeispiels verwendeten Zeichnungen zeigen:

Fig. 1	ein Blockdiagramm der Mitwirkenden in Transaktionen gemäss dem erfindungsgemässen System; und
Fig. 2	ein Flussdiagramm eines erfindungsgemässen Verfahrens zum Abwickeln von Transaktionen,

[0041] Grundsätzlich sind in den Figuren gleiche Elemente mit gleichen Bezugszeichen versehen.

Wege zur Ausführung der Erfindung

[0042] Das hier beschriebene Ausführungsbeispiel betrifft Transaktionen im Zusammenhang mit Wechseln bzw. Schuldscheindarlehen (Promissory Notes), namentlich Transaktionen zwischen Unternehmen (juristischen Personen). In einem solchen Wechsel verspricht eine Partei (der Aussteller), einer anderen Partei (dem Bezogenen) zu einem Fälligkeitszeitpunkt eine bestimmte Summe an diese andere Partei oder einen Dritten (Zahlungsempfänger) zu bezahlen.

[0043] Im Rahmen des beschriebenen Systems sind jeder der beteiligten Parteien (juristischen Personen) bestimmte Nutzer (natürliche Personen) zugeordnet, die im Namen der Parteien handeln können, d. h. bindend (virtuelle) Unterschriften im Rahmen der Transaktionen leisten können.

[0044] Die Figur 1 zeigt ein Blockdiagramm, in dem auf vereinfachte Weise die Mitwirkenden in solchen Transaktionen dargestellt sind. Dargestellt ist ein Nutzerunternehmen 10 mit einer natürlichen Person als Administrator 11 und mehreren natürlichen Personen als Nutzer 15.1, 15.2, 15.3.

[0045] Das Nutzerunternehmen 10 dient nur als Beispiel. In Transaktionen sind in der Regel mehrere solche Nutzerunternehmen involviert, die jeweils auch unterschiedliche Rollen wahrnehmen können. Alle Nutzerunternehmen sind auf dieselbe Art und Weise in das System eingebunden.

[0046] Weiter dargestellt ist das computergestützte System 100 des Dienstleisters, das u.a. einen Server 101 mit Kommunikationsschnittstellen und Rechnermitteln umfasst und eine private Blockchain 150, die vom Dienstleister selbst oder

im Auftrag des Dienstleisters von einem weiteren Dienstleister verwaltet wird. In der Blockchain sind in an sich bekannter Weise Daten in Datenblöcken gespeichert, wobei die Datenblöcke zwischen mehreren Rechnern eines Computernetzwerks repliziert, geteilt und synchronisiert sind.

[0047] Der Server 101 umfasst ein Verknüpfungsmodul 102, ein Berechtigungsmodul 103, ein Eingangsmodul 104, ein Überprüfungsmodul 105 und ein Aufzeichnungsmodul 106.

[0048] Weiter involviert ist eine Zertifizierungsstelle 200 zur Ausgabe von Identitätszertifikaten. Dabei handelt es sich im dargestellten Beispiel um Zertifikate für qualifizierte elektronische Signaturen (QES). Jedes der Zertifikate umfasst zwei oder mehr Zertifikate, welche miteinander verkettet sind, namentlich das Nutzerzertifikat der jeweiligen natürlichen Person, deren Identität bestätigt werden soll und eines oder mehrere damit verkettete Herausgeberzertifikate. Es können mehrere Zertifizierungsstellen vorgesehen sein, deren Zertifikate vom Dienstleister akzeptiert werden.

[0049] Das Nutzerunternehmen 10 bzw. der Administrator 11 und die Nutzer 15.1...3 interagieren mit der Zertifizierungsstelle 200 zum Erhalt von Identitätszertifikaten, die dem Administrator 11 bzw. den Nutzern 15.1...3 zugeordnet sind. Der Server 101 des Dienstleisters interagiert ebenfalls mit der Zertifizierungsstelle 200, z. B. zum Erhalt von Herausgeberzertifikaten.

[0050] Ein vereinfachtes Flussdiagramm eines erfindungsgemässen Verfahrens zum Abwickeln von Transaktionen ist in der Figur 2 dargestellt. Zunächst erhält das Verknüpfungsmodul 102 des Servers 101 von der Zertifizierungsstelle 200 ein Herausgeberzertifikat und speichert einen aus dessen öffentlichen Schlüssel abgeleiteten Fingerprint in der Blockchain 150 (Schritt 301).

[0051] Der Fingerprint wird aus den Daten des Zertifikats gewonnen, das beispielsweise im pem-Format vorliegt. Er wird beispielsweise durch die Anwendung einer SHA-256-Hashfunktion auf diese Daten gewonnen. Für die Gewinnung des Fingerprints geeignet ist beispielsweise der öffentliche Schlüssel (Public Key) des Zertifikats. Weitere Elemente können herangezogen werden.

[0052] Fingerprints von Identitätszertifikaten von Administratoren 11, verknüpft mit Angaben zum Nutzerunternehmen 10 (z. B. mit einer eindeutigen Firmenkennung bzw. Unternehmensnummer) werden vom Berechtigungsmodul 103 des Servers 101 in der Blockchain 150 abgelegt (Schritt 302). Der so erfasste Administrator 11 kann dann Nutzern 15.1...3 eine Berechtigung erteilen, um im Namen des Nutzerunternehmens 10 gegenüber dem Dienstleister zu handeln. Dazu signiert er eine Datenportion, die die eindeutige Kennung des zu berechtigenden Nutzers (serial number des entsprechenden Identitätszertifikats) umfasst und die Angabe der juristischen Person, für welche der Administrator und der Nutzer handeln (sollen). Das so erzeugte Berechtigungszertifikat überlässt er dem jeweiligen Nutzer 15.1...3 zu dessen Verwendung (Schritt 303).

[0053] Die berechtigten Nutzer 15.1...3 können dann mit dem Server 101 des Dienstleisters im Rahmen von Transaktionen zusammenwirken. Dazu übermitteln sie über das Eingangsmodul 104 des Servers 101 eine entsprechende Transaktionsanforderung an den Server 101, die u.a. durch den Nutzer signierte Datenportionen und das vom Administrator 11 erhaltene Berechtigungszertifikat umfasst (Schritt 304).

[0054] Bei sämtlichen Transaktionen wird vom Überprüfungsmodul 105 des Servers 101 nebst den Signaturen der signierenden Nutzer, unter Rückgriff auf den gespeicherten Fingerprint des Herausgeberzertifikats, auch geprüft, ob diese eine Berechtigung für die betroffene juristische Person haben (Schritt 305). Nach erfolgreicher Prüfung werden Daten über die Transaktionen bzw. die davon betroffenen Wechsel vom Aufzeichnungsmodul 106 ebenfalls in der Blockchain 150 gespeichert (Schritt 306).

[0055] Unterschriften der Nutzer werden durch eine Signaturstruktur mit folgenden Elementen repräsentiert:

1. Die Signatur des Nutzers, der den Wechsel unterzeichnet. Diese besteht aus einem vom Nutzer signierten Hash folgender Elemente:
   - dem Hash des Wechsels,
   - der Bezeichnung der juristischen Person des Nutzers und
   - einem Hash von allenfalls vorhandenen Bedingungen (Rabatte oder weitere Angaben, die im Wechsel nicht sichtbar sein, während der Unterzeichnung aber dennoch überprüfbar sein sollen);
2. einer Signatur eines Administrators der juristischen Person. Diese besteht aus einem vom Administrator signierten Hash folgender Elemente:
   - der eindeutigen laufenden Nummer des Nutzers und
   - der Bezeichnung der juristischen Person des Administrators und des Nutzers;
3. den Namen der juristischen Person.

[0056] Ein Wechsel (Promissory Note PN) wird im Rahmen des beschriebenen Systems durch eine Struktur mit folgenden Elementen repräsentiert:

1. Eine Hauptstruktur, die während der Lebensdauer des Wechsels unverändert bleibt, umfassend folgende Elemente:
   - die Angabe des Nominalwerts;
   - die Angabe der Währung;
   - die Angabe des Fälligkeitsdatums;
   - die Angabe möglicher Transferempfänger (juristische Personen) (optional);
   - eine Nonce (zur Verhinderung von Replay-Attacken);
   - eine Angabe der juristischen Person des Ausstellers;
   - eine Angabe der juristischen Person des Garantiegebers (optional);
   - fixe Metadaten;
2. einer Kennung;
3. einem Ausgabedatum;
4. einer Signaturenstruktur (siehe unten) mit den derzeitigen Signaturen;
5. Angaben zur Geschichte der PN (aktualisiert, wenn die PN erledigt, gelöscht oder übertragen wird);
6. eine Statusangabe (offen, fällig, erledigt, gelöscht, evtl. weitere);
7. die Angabe der juristischen Person des Inhabers und
8. veränderliche Metadaten, umfassend einfach und mehrfach veränderliche Daten.

[0057] Die Signaturenstruktur des Wechsels umfasst mehrere Signaturstrukturen und weitere Elemente wie folgt:

Element	Typ	Inhalt
Aussteller	Signatur	Hash (PN), jur. Person (LE), Hash (Bedingungen)
Bedingungen Ausstellung	String	Hash (Bedingungen Herausgabe)
Bedingungen Bürgschaft (Aval)	String	Hash (Bedingungen Bürgschaft)
Bedingungen Transfer	String	Hash (Bedingungen Transfer)
Garantiegeber	Signatur	Hash (PN), Hash (Bedingungen)
Inhaber (Bezogener)	Signatur	Hash (PN), LE Inhaber, LE neuer Inhaber (optional), Hash (Bedingungen)
neuer Inhaber	Signatur	Hash (PN), LE Inhaber, LE neuer Inhaber, Hash (Bedingungen)

[0058] Zur Ausstellung eines neuen Wechsels einigen sich der Aussteller und der (initiale) Inhaber auf den Hash der Angaben gemäss der Hauptstruktur (Punkt 1 oben) und die juristische Person des Inhabers. Dazu kommt allenfalls ein Hash von Daten, die zwischen den Parteien vereinbarte Bedingungen betreffen. Diese zwei bzw. drei Datenportionen werden sodann von Nutzern signiert, die für die beiden Parteien zur Unterzeichnung berechtigt sind.

[0059] Bei einer kombinierten Ausstellung und Übertragung muss der Aussteller dieselben Daten wie bei der Ausstellung signieren. Beim ursprünglichen und neuen Inhaber kommen zu den zu signierenden Daten jeweils noch die juristische Person des neuen Inhabers dazu und allenfalls Bedingungen für die Übertragung. Im Rahmen der Abwicklung des Transfers wird anhand der Promissory-Note-Strul<tur geprüft, ob die Übertragung des Wechsels eingeschränkt ist und falls ja, ob die vorgesehene Übertragung im Rahmen der Einschränkungen zulässig ist.

[0060] Ein Wechsel kann - insbesondere nach Leistung des vereinbarten Betrags durch den Aussteller - durch Antrag des (aktuellen) Inhabers erledigt werden. Dazu signiert der Inhaber eine Datenportion mit der Identifikationsnummer des Wechsels, dem Vermerk, dass der Wechsel erledigt ist und der juristischen Person des Inhabers. Es bedarf zur Erledigung keiner weiteren Unterschriften.

[0061] Im Rahmen des beschriebenen Systems ist eine Unterschrift gültig, wenn das entsprechende Zertifikat gültig ist, die Berechtigung der Unterzeichnenden nicht zurückgezogen wurde (siehe unten) und der unterzeichnende Nutzer über eine gültige Zugriffsberechtigung mit der handelnden, juristischen Person verknüpft ist. Ergänzend können hinterlegte Zeichnungsberechtigungen (z. B. betreffend kollektiver Zeichnungsberechtigung) geprüft werden. Entsprechend wird die Gültigkeit von Unterschriften im Rahmen des beschriebenen Systems gemäss folgenden Schritten geprüft, jeweils angewandt auf jede Unterschrift einer PN:

1. Die entsprechenden Zertifikatsdaten werden erhalten, sowohl für den unterzeichnenden Nutzer als auch für den zugeordneten Administrator.
2. Die Liste der erfassten Administratoren der der Signatur zugeordneten juristischen Person wird abgerufen.
3. Es wird geprüft, ob das Zertifikat des Nutzers von einem registrierten Herausgeber (Zertifizierungsstelle) stammt. Dazu wird anhand des Herausgeberzertifikats, das mit dem Identitätszertifikat des Nutzers verkettet ist, ein Fingerprint generiert. Dieser wird dann mit den Fingerprints verglichen, die in der Blockchain hinterlegt sind.
4. Es wird geprüft, ob der Nutzer nicht in einer Liste mit zurückgezogenen Zugriffsberechtigungen aufgeführt ist. Solche Listen sind in der Blockchain abgelegt und werden für jede juristische Person separat geführt, weil ein spezifischer Nutzer (natürliche Person) Zugriffsberechtigungen für mehrere juristische Personen haben kann und weil diese unabhängig voneinander verwaltet werden sollen.
5. Es wird geprüft, ob das Zertifikat des Nutzers eine Zugriffsberechtigung eines der erfassten Administratoren der juristischen Person umfasst und ob diese Zugriffsberechtigung gültig vom entsprechenden Administrator signiert wurde.

[0062] Weitere Prüfungen sind möglich, z. B. ob alle Unterschriften, die mit einer Partei einer Transaktion verknüpft sind, derselben juristischen Person zugeordnet sind, ob die Anzahl der Unterschriften ausreichend ist usw.

[0063] Die in der Blockchain gespeicherten Promissory Notes sind mit einem symmetrischen Schlüssel verschlüsselt, beispielsweise mittels AES-Verschlüsselung. Der Schlüssel (und gegebenenfalls auch ein Initialisierungsvektor) wird off-chain erzeugt und abgelegt. Er wird für den Zugriff auf die Promissory Note benötigt; wird er gelöscht, kann auf die Information der entsprechenden Promissory Note weder lesend noch schreibend mehr zugegriffen werden. Entsprechend verliert die Promissory Note jegliche Wirkung, und es ist trotz Speicherung der entsprechenden Daten in der Blockchain auch nicht mehr ersichtlich, was ihr Inhalt gewesen war.

[0064] Die Erfindung ist nicht auf das dargestellte Ausführungsbeispiel beschränkt. So können spezifische Aspekte des beschriebenen Systems und des beschriebenen Verfahrens anders ausgeführt sein. Die Erfindung lässt sich zudem nicht nur bei der Abwicklung von Transaktionen im Zusammenhang mit Wechseln oder anderen Finanzinstrumenten, sondern auch für andere Transaktionen verwenden.

[0065] Zusammenfassend ist festzustellen, dass die Erfindung einen Server, ein System und ein Verfahren schafft, die eine effiziente Abwicklung von Transaktionen bei sicherer Identifikation der Transaktionspartner ermöglichen.

Patentansprüche

1. Server zur Abwicklung von Transaktionen, wobei der Server zur Verbindung mit einem Computernetzwerk ausgebildet ist, das einen Distributed Ledger speichert, welcher eine Mehrzahl von Datenblöcken umfasst, die zwischen mehreren Rechnern des Computernetzwerks repliziert, geteilt und synchronisiert sind, und wobei der Server folgendes umfasst:
   a) ein Verknüpfungsmodul, das eingerichtet ist zum Empfangen eines öffentlichen Schlüssels einer Zertifizierungsstelle und zum Generieren und Speichern von Fingerprintdaten, die den öffentlichen Schlüssel repräsentieren, in einem der Datenblöcke des Distributed Ledger;
   b) ein Berechtigungsmodul, das eingerichtet ist zum Speichern von Zugriffsberechtigungen, die mit von der Zertifizierungsstelle ausgegebenen Identitätszertifikaten verknüpft sind, in einem der Datenblöcke des Distributed Ledger;
   c) ein Eingangsmodul, das eingerichtet ist zum Empfangen einer Transaktionsanforderung von einer anfordernden Stelle, wobei die Anforderung mit dem privaten Schlüssel der anfordernden Stelle signiert ist, der mit einem öffentlichen Schlüssel eines von der Zertifizierungsstelle ausgegebenen Identitätszertifikats der anfordernden Stelle verknüpft ist;
   d) ein Überprüfungsmodul, das eingerichtet ist zum Überprüfen einer Identität der anfordernden Stelle, gestützt auf die Anforderung der anfordernden Stelle, den gespeicherten Fingerprintdaten und den gespeicherten Zugriffsberechtigungen;

e) ein Aufzeichnungsmodul, das eingerichtet ist zum Aufzeichnen einer Transaktion, die der Transaktionsanforderung entspricht, in einem Datenblock des Distributed Ledger, sofern die Identität erfolgreich durch das Überprüfungsmodul verifiziert wurde.

2. Server zur Abwicklung von Transaktionen nach Anspruch 1, dadurch gekennzeichnet, dass das Berechtigungsmodul eingerichtet ist zum Speichern von Zuordnungen zu Identitätszertifikaten von Administratoren, dass das Eingangsmodul eingerichtet ist zum Empfangen von Transaktionsanforderungen, die ein Zugriffszertifikat mit einer Signatur eines Administrators umfassen, und dass das Überprüfungsmodul eingerichtet ist zur Prüfung, ob die Signatur des Administrators mit einem der Identitätszertifikate der gespeicherten Zugriffsberechtigungen verknüpft ist.

3. Server zur Abwicklung von Transaktionen nach Anspruch 2, dadurch gekennzeichnet, dass das Zugriffszertifikat eine eindeutige Kennung der anfordernden Stelle und eine Zuordnung zu einer Entität umfasst.

4. Computergestütztes System für die Abwicklung von Transaktionen, umfassend:
a) eine Zertifizierungsstelle zur Ausgabe von Identitätszertifikaten, wobei die Identitätszertifikate einen öffentlichen Schlüssel und eine Identität umfassen und von der Zertifizierungsstelle signiert sind;
b) ein Computernetzwerk, das einen Distributed Ledger speichert, welcher eine Mehrzahl von Datenblöcken umfasst, die zwischen mehreren Rechnern des Computernetzwerks repliziert, geteilt und synchronisiert sind;
c) einen Server zur Abwicklung von Transaktionen nach einem der Ansprüche 1 bis 3.

5. Verfahren zur Abwicklung von Transaktionen, umfassend die folgenden Schritte:
a) Speichern von Fingerprintdaten, die den öffentlichen Schlüssel einer Zertifizierungsstelle repräsentieren, in einem einer Mehrzahl von Datenblöcken eines Distributed Ledger, wobei die Mehrzahl von Datenblöcken zwischen mehreren Rechnern eines Computernetzwerks repliziert, geteilt und synchronisiert sind;
b) Speichern von Zugriffsberechtigungen, die mit von der Zertifizierungsstelle ausgegebenen Identitätszertifikaten verknüpft sind, in einem der Mehrzahl von Datenblöcken des Distributed Ledger;
c) Empfangen einer Transaktionsanforderung einer anfordernden Stelle, wobei die Anforderung mit dem privaten Schlüssel der anfordernden Stelle signiert ist, der mit einem öffentlichen Schlüssel eines von der Zertifizierungsstelle ausgegebenen Identitätszertifikats der anfordernden Stelle verknüpft ist;
d) Überprüfung einer Identität der anfordernden Stelle, gestützt auf die Anfrage der anfordernden Stelle, den gespeicherten Fingerprintdaten und den gespeicherten Zugriffsberechtigungen;
e) Aufzeichnen einer Transaktion, die der Transaktionsanforderung entspricht, in einem Datenblock des Distributed Ledger, sofern die Identität erfolgreich durch das Überprüfungsmodul verifiziert wurde.

6. Verfahren nach Anspruch 5, dadurch gekennzeichnet, dass
den Zugriffsberechtigungen Identitätszertifikate von Administratoren zugeordnet sind,
die Transaktionsanforderung der anfordernden Stelle ein Zugriffszertifikat mit einer Signatur eines Administrators umfasst, und dass
eine erfolgreiche Überprüfung der Identität voraussetzt, dass die Signatur des Administrators mit einem der Identitätszertifikate der gespeicherten Zugriffsberechtigungen verknüpft ist.

7. Verfahren nach Anspruch 6, dadurch gekennzeichnet, dass das Zugriffszertifikat eine eindeutige Kennung der anfordernden Stelle und eine Zuordnung zu einer Entität umfasst.

8. Verfahren nach einem der Ansprüche 5 bis 7, dadurch gekennzeichnet, dass die Überprüfung der Identität der anfordernden Stelle eine Überprüfung umfasst, ob die anfordernde Stelle nicht in einer Widerrufsliste aufgeführt ist, die in einem Datenblock des Distributed Ledgers gespeichert ist.

9. Verfahren nach einem der Ansprüche 5 bis 8, dadurch gekennzeichnet, dass die Transaktion vor der Aufzeichnung unter Verwendung einer symmetrischen Verschlüsselung verschlüsselt wird und dass Transaktionen durch Löschen eines Ver-/Entschlüsselungsschlüssels verworfen werden können.

10. Verfahren nach einem der Ansprüche 5 bis 9, dadurch gekennzeichnet, dass die Transaktionsanforderung von zusätzlichen Parteien unterzeichnet ist, die an der aufzuzeichnenden Transaktion beteiligt sind, und dass die Identität der zusätzlichen Parteien auf der Grundlage der jeweiligen gespeicherten Fingerprintdaten und gespeicherten Zugriffsberechtigungen überprüft wird.

11. Verfahren nach einem der Ansprüche 5 bis 10, dadurch gekennzeichnet, dass das Speichern der Zugriffsberechtigungen in einem Datenblock zusatzlich von einer Identitätsprüfung abhängig ist, die unabhängig ist vom Identitätszertifikat.

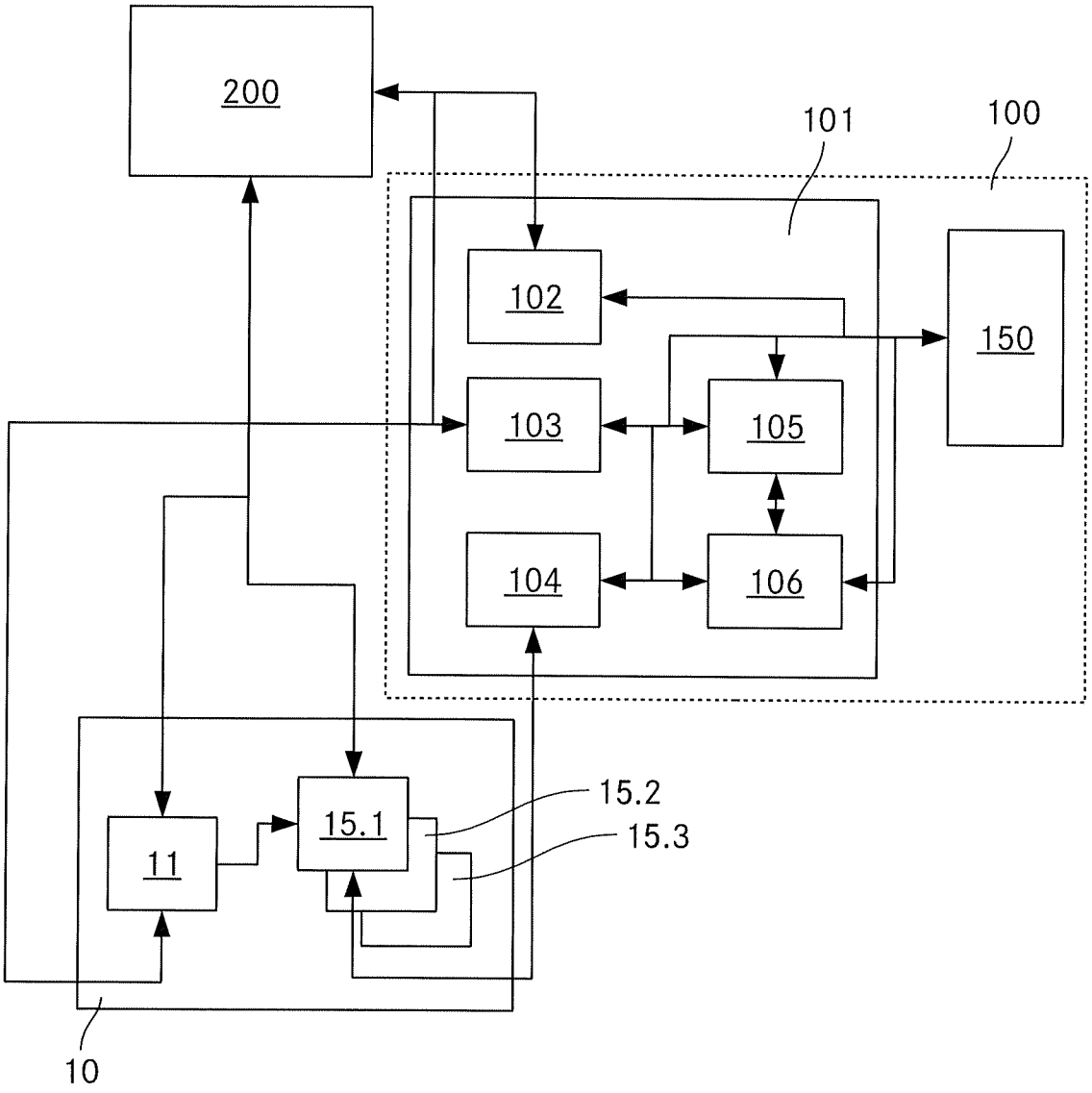


Fig. 1

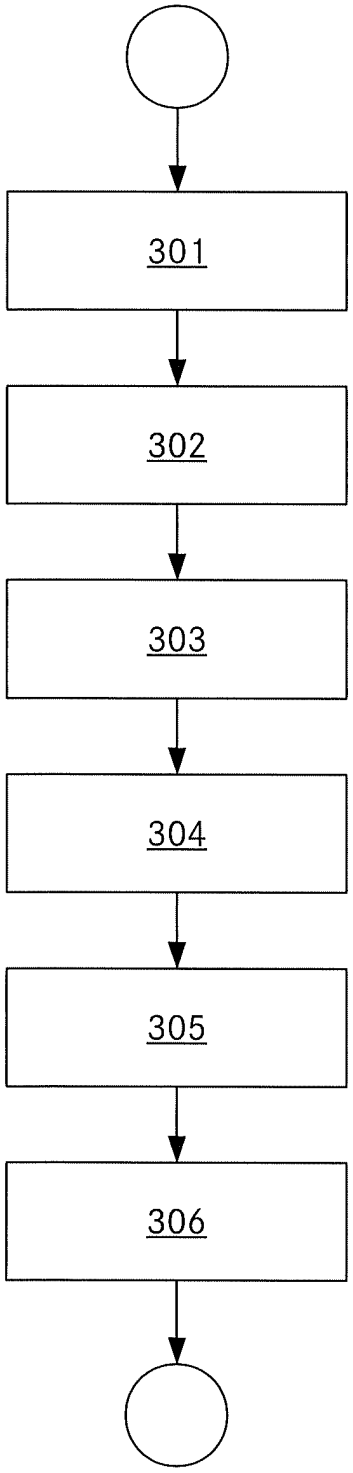


Fig. 2