(19) Deutsches Patent- und Markenamt

(10) **DE 10 2020 213 240 A1** 2022.04.21

(12) # Offenlegungsschrift

(21) Aktenzeichen: **10 2020 213 240.2**
(22) Anmeldetag: **20.10.2020**
(43) Offenlegungstag: **21.04.2022**

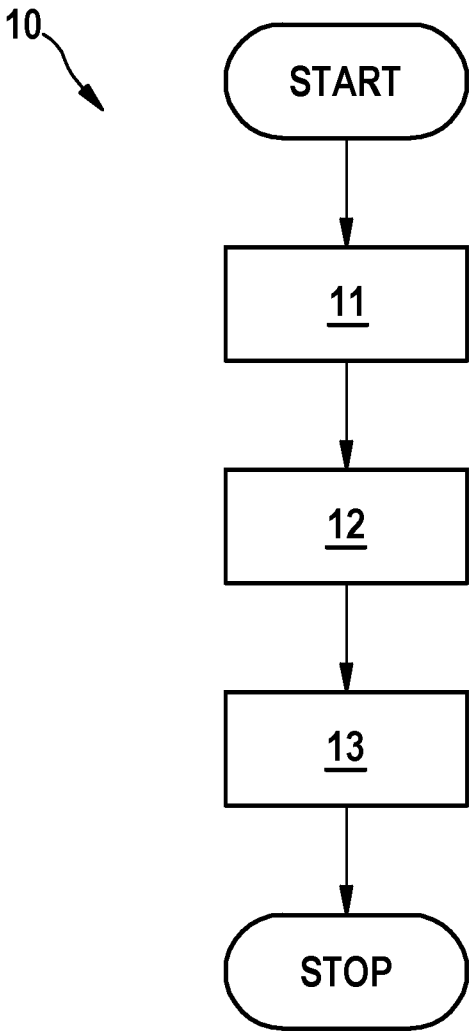
(51) Int Cl.: ***G06F 21/64*** (2013.01)
G06F 16/16 (2019.01)
G06Q 20/36 (2012.01)

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

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

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen.

(54) Bezeichnung: **Verfahren und Vorrichtung zum Abwickeln einer Transaktion zwischen mehreren Partitionen einer Blockkette**



(57) Zusammenfassung: Verfahren (10) zum Abwickeln einer Transaktion zwischen mehreren Partitionen einer Blockkette, gekennzeichnet durch folgende Merkmale:
- auf den Partitionen werden intelligente Verträge bereitgestellt (1),
- durch die Verträge werden Zustandskanäle in den Partitionen verankert (2) und
- die Transaktion zwischen den Partitionen wird auf den Zustandskanälen ausgeführt (3).

Beschreibung

[0001] Die vorliegende Erfindung betrifft ein Verfahren zum Abwickeln einer Transaktion zwischen mehreren Partitionen einer Blockkette. Die vorliegende Erfindung betrifft darüber hinaus eine entsprechende Vorrichtung, ein entsprechendes Computerprogramm sowie ein entsprechendes Speichermedium.

Stand der Technik

[0002] Als dezentrales Transaktionssystem, Transaktionsdatenbank oder verteiltes Hauptbuch (distributed ledger) wird jegliches Protokoll in Rechnernetzen bezeichnet, das eine Übereinkunft (consensus) hinsichtlich der Abfolge bestimmter Transaktionen herbeiführt. Eine häufige Ausprägung eines solchen Systems beruht auf einer Blockkette (blockchain) und bildet die Grundlage zahlreicher sogenannter Kryptowährungen.

[0003] Das nach dem Stand der Technik am häufigsten benutzte Konsensverfahren sieht einen Arbeitsnachweis (proof of work, PoW) für die Erzeugung neuer gültiger Blöcke vor. Um einem übermäßigen Energieverbrauch durch die Erbringung derartiger Nachweise sowie einem unnötigen Anwachsen der Blockkette entgegenzuwirken, wurden sogenannte Transaktions- oder Zustandskanäle (state channels) vorgeschlagen und verallgemeinert, die einzelne Teilnehmer abseits der Blockkette (off chain) verbinden, gleichwohl in letzterer verankert sind. Einen Überblick dieser Technologie bietet COLEMAN, Jeff; HORNE, Liam; XUANJI, Li. Counterfactual: Generalized state channels. 2018.

[0004] DE102018210224A1 offenbart in der Ausführungsform gemäß Anspruch 6 folgendes Verfahren zum Vereinbaren einer Zusammenarbeit zwischen zwei Systemen: Das erste System sendet seine Annahmen bezüglich des zweiten Systems und seine diesem gewährten Garantien; umgekehrt sendet das zweite System dessen Annahmen bezüglich des ersten Systems und jenem gewährten Garantien. Eine Transaktionsdatenbank empfängt diese wechselseitigen Annahmen und Garantien, prüft, ob sie einander entsprechen, setzt gegebenenfalls einen zwischen den Systemen zu schließenden digitalen Sicherheitsvertrag auf und dokumentiert diesen schließlich, indem es einer Blockkette einen entsprechenden Block hinzufügt. Es sendet den Block mit dem Sicherheitsvertrag daraufhin an beide Systeme, welche die Zusammenarbeit aufnehmen, sobald sie den Block empfangen. Diese etablieren hierzu einen wechselseitigen Transaktionskanal, auf welchem sie nach Empfang des Blockes Informationen und unterschriebene Mitteilungen austauschen. Wenn eines der Systeme eine den Sicherheitsvertrag verletzende Information empfängt, ersucht es die Transaktionsdatenbank um Schlichtung. Die Transaktionsdatenbank setzt das andere System hiervon in Kenntnis, fordert von diesem die - vermeintlich den Sicherheitsvertrag verletzende - Information an und prüft letztere anhand des Vertrages.

[0005] Derlei intelligente Verträge (smart contracts) verkörpern die rechtsgeschäftliche Logik jedweder verteilten Anwendung (distributed application, dApp) einer Transaktionsdatenbank. DE102017214902A1 beispielsweise beschreibt einen intelligenten Vertrag zum Vorbereiten und/oder Ausführen von Transaktionen zwischen einem Halter eines Endgeräts und einem Dienstleistungsanbieter, wobei der intelligente Vertrag Bedingungen des Dienstleistungsanbieters für Dienstleistungen eines Informationsdienstleistungsanbieters, insbesondere Bedingungen über Benutzungsgebühren, vorzugsweise eine Straßenbenutzungsgebühr, und/oder für Dienstleistungen eines Servicedienstleistungsanbieters, insbesondere Bedingungen über Überlassungsgebühren, vorzugsweise über Parkgebühren, Tankgebühren, Gebühren einer Ladestation für das Endgerät und/oder Bedingungen einer Versicherung und/oder Bedingungen über Nutzungsgebühren, vorzugsweise über Gebühren einer gemeinschaftlichen Nutzung des Endgeräts zum Bereitstellen und/oder Abbrechen für eine Dienstleistung und/oder von dem Halter für dieses Endgerät definierte Bedingungen für eine Annahme und/oder eine Beendigung der Dienstleistung enthält, wobei der intelligente Vertrag in einem Berechtigungsknoten eines auf einer Blockchain basierten Computernetzwerks ausgeführt wird.

[0006] Die herkömmlicherweise zur Denormalisierung in Datenbankanwendungen genutzte horizontale Fragmentierung (sharding) kann dazu dienen, schnell anwachsende Blockketten in unabhängige Partitionen (shards) aufzuteilen. Diesen Ansatz erläutert LUU, Loi, et al. A secure sharding protocol for open blockchains. In: Proceedings ofthe 2016 ACM SIGSAC Conference on Computer and Communications Security. 2016. S. 17-30.

Offenbarung der Erfindung

[0007] Die Erfindung stellt ein Verfahren zum Abwickeln einer Transaktion zwischen mehreren solchen Partitionen einer Blockkette, eine entsprechende Vorrichtung, ein entsprechendes Computerprogramm sowie ein entsprechendes maschinenlesbares Speichermedium gemäß den unabhängigen Ansprüchen bereit.

[0008] Der erfindungsgemäße Ansatz beruht auf einer Betrachtung von Shards als parallel verlaufenden Ketten mit der Möglichkeit, Wechselwirkungen zwischen den Ketten, also zwischen Shards (cross-shard), in einer ganzheitlich abgesicherten Weise auszuüben.

[0009] Transaktionen auf unabhängigen Shards können problemlos parallelisiert und die Anzahl der Shards zur Laufzeit angepasst werden.

[0010] Allerdings erfordern Shard-übergreifende Transaktionen, z. B. die Übertragung eines Zustandswertes von einem auf einen anderen Shard, eine koordinierte Abwicklung auf allen betroffenen Shards; beispielsweise würde die Übertragung eines auf einem Shard gespeicherten Wertes, aufgeteilt in zwei Beträge, an zwei Zieladressen auf zwei verschiedenen Shards eine Transaktion mit drei Shards erfordern.

[0011] Diese Transaktionen mit mehreren Shards verringern Effizienz und Durchsatz des Systems und erhöhen dessen Kosten aufgrund des auf verschiedenen Shards erforderlichen Schürfens (mining).

[0012] Daher sind auch die für den Nutzer anfallenden Kosten in der Regel so bemessen, dass sich diese nachteiligen Auswirkungen von Transaktionen mit mehreren Shards im Preis niederschlagen, letzterer also mit der Anzahl betroffener Shards steigt.

[0013] Das vorgeschlagene Verfahren begegnet diesen mit Transaktionen zwischen Shards verbundenen Mehrkosten durch eine Anwendung vertrauensfreier Kanalstrukturen auf Shards. Durch eine erfindungsgemäße Verankerung intelligenter Verträge in den betreffenden Shards lassen sich derartige Transaktionen auf effiziente, aber dennoch sichere Weise abseits der Blockkette ohne die Voraussetzung einer Vertrauensbasis zwischen den Beteiligten abwickeln.

[0014] Durch die in den abhängigen Ansprüchen aufgeführten Maßnahmen sind vorteilhafte Weiterbildungen und Verbesserungen des im unabhängigen Anspruch angegebenen Grundgedankens möglich.

Figurenliste

[0015] Ausführungsbeispiele der Erfindung sind in den Zeichnungen dargestellt und in der nachfolgenden Beschreibung näher erläutert. Es zeigt:

Fig. 1 das Flussdiagramm eines Verfahrens gemäß einer ersten Ausführungsform.

Fig. 2 schematisch ein Steuergerät gemäß einer zweiten Ausführungsform.

Ausführungsformen der Erfindung

[0016] **Fig. 1** illustriert den grundlegenden Ablauf eines erfindungsgemäßen Verfahrens (10) zum Abwickeln einer Transaktion zwischen mehreren Partitionen oder Shards einer Blockkette. Dieses Prinzip soll anhand eines einfachen Beispiels veranschaulicht werden, welches sich ohne Weiteres verallgemeinern lässt.

[0017] Angenommen sei hierzu ein dezentrales Transaktionssystem mit Nutzern U_1 bis U_N, die auf N verschiedenen Shards aktiv sind, also Adressen und diesen zugeordnete Guthaben auf jeweils einem dieser Shards besitzen. Angenommen sei ferner, U_i wünsche einen Zustandswert an einen anderen Nutzer U_j zu übertragen, womit eine Shard-übergreifende Transaktion einherginge.

[0018] Wir nutzen nun die Einsicht, dass, wie bei vertrauensfreien Kanälen, Kanalnetzen, Netzknoten usw. üblich, Transaktionskosten in der Kette (on chain) durch den Einsatz mehrerer Hilfsverträge vermieden werden können, die eine sichere Verankerung der außerhalb der Kette getätigten Transaktionen ermöglichen, beispielsweise unter Zugänglichmachung von Inhaber- und Entscheidungsfunktionen der Kette.

[0019] In einem ersten Ansatz werden diese Verträge für jeden Shard bereitgestellt (Prozess 11).

[0020] Vorausgesetzt sei eine auf zwei oder mehr, insbesondere sämtlichen, Shards aktive Vermittlerin Ingrid. Diese Vermittlerin kann nun einen Zustandskanal zu U_i in Shard i und U_j in Shard j verankern (Prozess 12). In Anwendung der üblichen Zustandskanal-Ansätze kann nun ein Transfer von U_i zu U_j über Ingrid durch ein Zusammenwirken der drei Beteiligten außerhalb der Kette ausgeführt werden (Prozess 13), sofern keine Streitbeilegung erforderlich ist.

[0021] Zusammengefasst überträgt U_i den Wert an Ingrid auf Shard i unter der Bedingung, dass Ingrid den gleichen Betrag an U_j auf Shard j überträgt. Dies kann auf verschiedenen aus dem Stand der Technik bekannten Wegen erreicht werden.

[0022] Somit sind keine On-Chain-Interaktion und insbesondere keine Cross-Shard-Transaktion erforderlich, sofern alle Beteiligten übereinstimmen und ein Schiedsverfahren entbehrlich ist.

[0023] Im Rahmen der bekannten Möglichkeiten mehrfach verschachtelter, gestapelter (virtueller) Kanäle können flexible und leistungsfähige Netze für einen effizienten Transfer über die Shards hinweg aufgebaut werden, wie es in einem Shardbasierten System üblich ist. Beispielsweise können Knotenpunkte auf vielen oder gar sämtlichen Shards, indirekte Verbindungen (multi-hop) über mehrere mittelgroße Knotenpunkte bis hin zu einfachen Multi-Hop--Verbindungen zwischen gleichrangigen Knoten (peer to peer) vorgesehen sein.

[0024] Der anfängliche Aufwand für die Bereitstellung (11) der zur Verankerung (12) erforderlichen Hilfsverträge und das Anlegen der On-Chain-Kanäle auf den Shards wird durch die drastisch reduzierten Kosten für die Ausführung (13) von Cross-Shard-Transaktionen schnell amortisiert.

[0025] Um den Unterschied zu herkömmlichen Lösungen zu verdeutlichen, sei darauf hingewiesen, dass nach dem Stand der Technik alle Nutzer und Vermittler bzw. Hubs auf dem gleichen Shard aktiv sein müssten. Dies würde allenfalls eine Senkung der On-Chain-Kosten für Transaktionen innerhalb dieses Shards ermöglichen.

[0026] Im Gegensatz dazu erlaubt der vorliegende Ansatz die effiziente Überbrückung von Shards auf der Grundlage sicherer Konstrukte, wie sie bei vertrauensfreien Kanälen zur Anwendung kommen.

[0027] In einem zweiten Ansatz könnte das verteilte System, das die Shards betreibt und gegebenenfalls zur Laufzeit automatisch weitere Shards hinzufügt, die Hilfsverträge für die Verankerung des Zustandskanals im Rahmen der Einrichtung eines neuen Shards bereitstellen (11), sodass die On-Chain-Kanäle eröffnet und zur Ausführung (13) der Off--Chain-Transaktionen auch für neue Shards genutzt werden können, ohne dass die Hilfsverträge aktiv bereitgestellt werden müssen.

[0028] Nach einem dritten Ansatz werden die Hilfsverträge zur Verankerung (12) der Zustandskanäle nicht für jeden Shard einzeln, sondern gemeinsam für alle Shards in Form einer allgemein nutzbaren Funktionalität bereitgestellt (11).

[0029] Dies wiederum erlaubt es, On-Chain-Kanäle zur Verankerung (12) anzulegen und die Off--Chain-Transaktionen auch für neue Shards darauf auszuführen (13), ohne dass die Hilfsverträge aktiv bereitgestellt werden müssten.

[0030] Die Vermittler- bzw. Knotenpunkt-Funktion könnte wie oben beschrieben von jedem Nutzer übernommen werden, der auf mehr als einem Shard aktiv ist. Darüber hinaus könnte das verteilte System selbst entsprechende Möglichkeiten bieten.

[0031] Dieses Verfahren (10) kann beispielsweise in Software oder Hardware oder in einer Mischform aus Software und Hardware beispielsweise in einem Steuergerät (20) implementiert sein, wie die schematische Darstellung der **Fig. 2** verdeutlicht.

ZITATE ENTHALTEN IN DER BESCHREIBUNG

Zitierte Patentliteratur

- DE 102018210224 A1 [0004]
- DE 102017214902 A1 [0005]

Patentansprüche

1. Verfahren (10) zum Abwickeln einer Transaktion zwischen mehreren Partitionen einer Blockkette, **gekennzeichnet durch** folgende Merkmale:
- auf den Partitionen werden intelligente Verträge bereitgestellt (11),
- durch die Verträge werden Zustandskanäle in den Partitionen verankert (12) und
- die Transaktion zwischen den Partitionen wird auf den Zustandskanälen ausgeführt (13).

2. Verfahren (10) nach Anspruch 1, **gekennzeichnet durch** folgendes Merkmal:
- das Bereitstellen (11) erfolgt durch einen auf mehreren der Partitionen aktiven Vermittler.

3. Verfahren (10) nach Anspruch 2, **gekennzeichnet durch** folgendes Merkmal:
- der Vermittler ist ein mit weiteren Vermittlern in der Blockkette vernetzter Knotenpunkt.

4. Verfahren (10) nach Anspruch 2, **gekennzeichnet durch** folgendes Merkmal:
- die Vermittler sind indirekt über mehrere Partitionen verbunden.

5. Verfahren (10) nach Anspruch 1, **gekennzeichnet durch** folgende Merkmale:
- die Partitionen werden von einem in der Blockkette verteilten System betrieben und
- das Bereitstellen (11) erfolgt durch das System.

6. Verfahren (10) nach Anspruch 5, **gekennzeichnet durch** folgendes Merkmal:
- das Bereitstellen (11) erfolgt, wenn das System weitere Partitionen der Blockkette einrichtet.

7. Verfahren (10) nach Anspruch 1, **gekennzeichnet durch** folgendes Merkmal:
- das Bereitstellen (11) erfolgt in Form einer durch sämtliche Partitionen gemeinsam nutzbaren Funktionalität.

8. Computerprogramm, welches eingerichtet ist, das Verfahren (10) nach einem der Ansprüche 1 bis 7 auszuführen.

9. Maschinenlesbares Speichermedium, auf dem das Computerprogramm nach Anspruch 8 gespeichert ist.

10. Vorrichtung (20), die eingerichtet ist, das Verfahren (10) nach einem der Ansprüche 1 bis 7 auszuführen.

Es folgt eine Seite Zeichnungen

Anhängende Zeichnungen

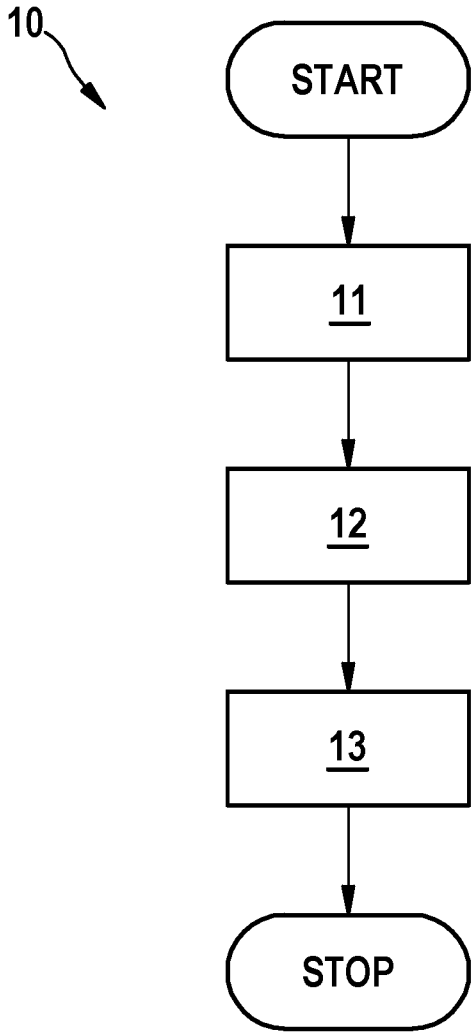


Fig. 1

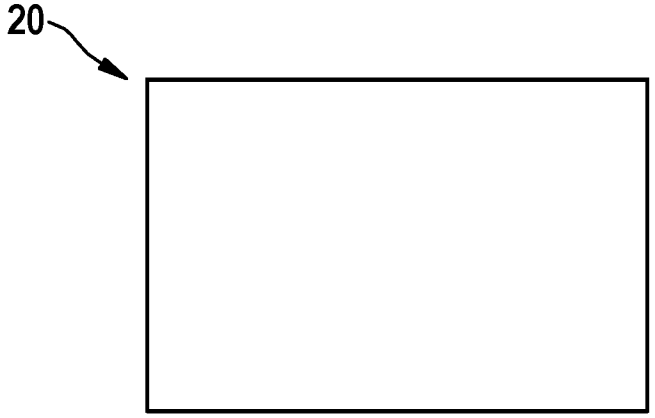


Fig. 2

