(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国 际 局

(43) 国际公布日
2019 年 4 月 18 日 (18.04.2019)

WIPO | PCT

(10) 国际公布号
WO 2019/072136 A1

(51) 国际专利分类号:
H04L 9/32 (2006.01) *G06Q 20/40* (2012.01)

(21) 国际申请号: PCT/CN2018/109246

(22) 国际申请日: 2018 年 10 月 5 日 (05.10.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201710951045.0 2017年10月13日 (13.10.2017) CN

(71) 申请人: 中国银联股份有限公司 (CHINA UNIONPAY CO., LTD.) [CN/CN]; 中国上海市浦东新区含笑路 36 号银联大厦, Shanghai 200135 (CN)。

(72) 发明人: 朱涛 (ZHU, Tao); 中国上海市浦东新区含笑路36号银联大厦7楼, Shanghai 200135 (CN)。
郑建宾 (ZHENG, Jianbin); 中国上海市浦东新区含笑路36号银联大厦7楼, Shanghai 200135 (CN)。
周钰 (ZHOU, Yu); 中国上海市浦东新区含笑路36号银联大厦7楼, Shanghai 200135 (CN)。

(74) 代理人: 中国专利代理 (香港) 有限公司 (CHINA PATENT AGENT (HK) LTD.); 中国香港特别行政区香港湾仔港湾道23号鹰君中心22字楼, Hong Kong (CN)。

(81) 指定国 (除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB,

(54) **Title:** BLOCKCHAIN NETWORK AND TRANSACTION METHOD THEREFOR

(54) **发明名称:** 区块链网络及其交易方法

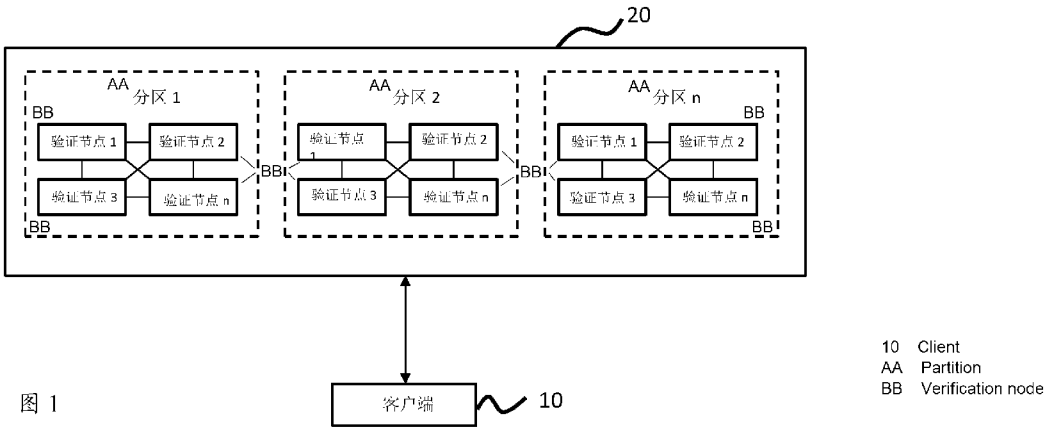

图 1

(57) **Abstract:** Provided by the present invention is a blockchain network, the network comprising: multiple verification nodes, a first portion of said multiple verification nodes being divided into a first partition, and a second portion of said multiple verification nodes being divided into a second partition, wherein said division is performed on the basis of service scenarios and groups or service vertical fields; verification nodes within said first partition are configured to verify a first transaction request from a client, sign said first transaction request once verification has been passed, and return the same to said client; and verification nodes in said second partition are configured to verify a second transaction request from said client, and record the same in an account log once verification has been passed. The present invention further provides a blockchain network-based transaction method and a computer storage medium.

(57) **摘要**: 本发明提供一种区块链网络, 所述网络包括: 多个验证节点, 所述多个验证节点中的第一部分被划分为第一分区, 所述多个验证节点中的第二部分被划分为第二分区, 其中, 所述划分基于业务场景、群体或业务垂直领域而进行, 所述第一分区内的验证节点配置成对来自客户端的第一交易请求进行验证, 并在验证通过后对所述第一交易请求进行签名, 并返回所述客户端; 以及所述第二分区内的验证节点配置成对来自所述客户端的第二交易请求进行验证, 并在验证通过后记入账本。本发明还提供了一种基于区块链网络的交易方法和计算机存储介质。

WO 2019/072136 A1

[见续页]

GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) **指定国**(除另有指明，要求每一种可提供的地区保护)：ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告(条约第21条(3))。

区块链网络及其交易方法

技术领域

本发明涉及区块链技术领域，特别涉及一种区块链网络及其交易方法。

背景技术

区块链是分布式数据存储、点对点传输、共识机制、加密算法等计算机技术的新型应用模式。所谓共识机制是区块链系统中实现不同节点之间建立信任、获取权益的数学算法。区块链的设计是一种保护措施，比如（应用于）高容错的分布式计算系统。区块链使混合一致性成为可能。这使区块链适合记录事件、标题、医疗记录和其他需要收录数据的活动、身份识别管理，交易流程管理和出处证明管理。区块链对于金融有巨大的潜能，对于引领全球贸易有着巨大的影响。

申请号为 201110058800.5、发明名称为："一种可并发和断续分析的日志事件关联分析方法和装置"的中国专利申请提供了一种可并发和断续分析的日志事件关联分析方法和装置。该装置需要对所有日志进行事后采集、分析（即事后审计），所有日志之间不存在内在联系。也就是说，在交易进行过程中不存在即时审计。当网络内存在恶意节点的情况下，该节点可能会伪造大量无效交易、对非法交易进行验证等作弊和不作为行为，这些恶意行为不能被及时察觉可能会造成区块链系统无法稳定的运行。

因此，期望一种改进的区块链网络及其交易方法。

以上公开于本发明背景部分的信息仅仅旨在增加对本发明的总体背景的理解，而不应当被视为承认或以任何形式暗示该信息构成已为本领域一般技术人员所公知的现有技术。

发明内容

为了解决以上提及的一个或多个问题，本发明提出一种多分区的

区块链网络，每个分区可设有分区标识，并且在验证交易过程中均可作为 Query 分区或者 Commit 分区。此外，本发明提出一种基于日志哈希链的设计方案，即一笔交易经 Query 及 Commit 分区（不同分区）分别验证后，会记录至节点自身的日志哈希链，该链全网可见，其中记录了该节点在系统运行过程中的所有行为，并且该哈希链的链头值将以签名的形式发送至网络内其他节点，最终实现网络内节点行为的交叉验证。本发明还提出一种时间区块链系统可审计性的方法及系统，其通过网络内节点间的互相审计和管理来实现（属于交易即时审计），并通过哈希算法来保证记录的不可篡改性。

根据本发明的一个方面，提供了一种区块链网络，该区块链网络包括：多个验证节点，所述多个验证节点中的第一部分被划分为第一分区，所述多个验证节点中的第二部分被划分为第二分区，其中，所述划分基于业务场景、群体或业务垂直领域而进行，所述第一分区内的验证节点配置成对来自客户端的第一交易请求进行验证，并在验证通过后对所述第一交易请求进行签名，并返回所述客户端；以及所述第二分区内的验证节点配置成对来自所述客户端的第二交易请求进行验证，并在验证通过后记入账本，其中所述第一交易请求包括交易内容，以及所述第二交易请求包括所述交易内容和所述客户端收集的所述第一分区内的验证节点的签名。

在上述区块链网络中，所述第一分区内的验证节点配置成在收到所述第一交易请求后，针对所述交易内容中的用户的数字签名、输入是否双花进行验证。

在上述区块链网络中，所述第二分区内的验证节点配置成判断所述第二交易请求中的交易是否得到所述第一分区内半数以上的验证节点的签名。

在上述区块链网络中，所述第一分区内的验证节点是请求节点，其配置成在验证通过后，以 Query(node, tx, input, timestamp)的形式记入日志，其中 node 为当前验证节点序号，tx 为交易哈希值，input 为验证节点验证通过的交易输入，timestamp 为当前时间戳。

在上述区块链网络中，所述第二分区内的验证节点为确认节点，

其配置成在验证通过后，以 Commit (node, tx, signs, timestamp)的形式记入日志，其中 node 为当前验证节点序号，tx 为交易哈希值，signs 为验证节点收到的所有签名，timestamp 为当前时间戳。

在上述区块链网络中，所述多个验证节点中的每一个具有其自身的日志哈希链，用于记录其在共识协议中的请求和/或确认行为。

根据本发明的另一个方面，提供了一种基于区块链网络的交易方法，所述区块链网络包括多个验证节点，所述多个验证节点中的第一部分被划分为第一分区，所述多个验证节点中的第二部分被划分为第二分区，所述划分基于业务场景、群体或业务垂直领域而进行，所述方法包括：所述第一分区内的验证节点对来自客户端的第一交易请求进行验证；在验证通过后，所述第一分区内的验证节点对所述第一交易请求进行签名，并返回所述客户端；所述第二分区内的验证节点对来自所述客户端的第二交易请求进行验证；以及在验证通过后，所述第二分区内的验证节点将交易信息记入账本，其中所述第一交易请求包括交易内容，以及所述第二交易请求包括所述交易内容和所述客户端收集的所述第一分区内的验证节点的签名。

在上述方法中，所述第一分区内的验证节点对来自客户端的第一交易请求进行验证包括：在收到所述第一交易请求后，所述第一分区内的验证节点针对所述交易内容中的用户的数字签名、输入是否双花进行验证。

在上述方法中，所述第二分区内的验证节点对来自所述客户端的第二交易请求进行验证包括：所述第二分区内的验证节点判断所述第二交易请求中的交易是否得到所述第一分区内半数以上的验证节点的签名。

在上述方法中，在验证通过后，所述第一分区内的验证节点对所述第一交易请求进行签名，并返回所述客户端包括：所述第一分区内的验证节点在验证通过后，以 Query(node, tx, input, timestamp)的形式记入日志，其中 node 为当前验证节点序号，tx 为交易哈希值，input 为验证节点验证通过的交易输入，timestamp 为当前时间戳。

在上述方法中，在验证通过后，所述第二分区内的验证节点将交

易信息记入账本包括：所述第二分区内的验证节点在验证通过后，以Commit (node, tx, signs, timestamp)的形式记入日志，其中 node 为当前验证节点序号，tx 为交易哈希值，signs 为验证节点收到的所有签名，timestamp 为当前时间戳。

在上述方法中，所述多个验证节点中的每一个具有其自身的日志哈希链，用于记录其在共识协议中的请求和/或确认行为。

根据本发明的又一个方面，提供了一种计算机存储介质，所述介质包括指令，所述指令在被执行时，实现如前所述的方法。

本发明的技术方案提出基于区块链网络节点分区的交易方法及系统，以分区的方式提高系统的交易处理能力。此外，区块链系统网络内节点的行为可通过对日志数据进行系统分析处理，形成节点间相互审计，形成各节点行为的互相见证（或交叉验证）。

通过纳入本文的附图以及随后与附图一起用于说明本发明的某些原理的具体实施方式，本发明的方法和装置所具有的其它特征和优点将更为具体地变得清楚或得以阐明。

附图说明

图 1 示意示出了本发明的一个实施例的基于区块链网络的交易系统架构图；

图 2 示意示出了本发明的一个实施例的基于区块链网络的交易系统架构图；

图 3 示意示出了本发明的一个实施例的基于区块链网络的交易方法；以及

图 4 示意示出了本发明的一个实施例的基于区块链网络的交易方法；以及

图 5 示意示出了根据本发明的一个实施例的日志哈希链。

具体实施方式

以下说明描述了本发明的特定实施方式以教导本领域技术人员如何制造和使用本发明的最佳模式。为了教导发明原理，已简化

或省略了一些常规方面。本领域技术人员应该理解源自这些实施方式的变型将落在本发明的范围内。本领域技术人员应该理解下述特征能够以各种方式接合以形成本发明的多个变型。由此，本发明并不局限于下述特定实施方式，而仅由权利要求和它们的等同物限定。

区块链系统中的可扩展性（Scalability）解决方案之于区块链的重要性，可类比于 TCP/IP 协议之于互联网的重要性。类似比特币区块链交易频率约 6.67 次/秒，每次交易需要 6 个区块确认，10 分钟才能产生一个区块，全网确认一次交易至少需要 1 个小时，这在很多应用场景下是很难接受的。为了解决这个问题，本发明从交易验证的方式作为切入点，通过分片处理的机制（sharding），即每个节点只处理一部分交易，比如一部分账户发起的交易，从而减轻节点的计算和存储负担，有效提高系统的交易吞吐量和交易时延。

图 1 示意示出了本发明的一个实施例的基于区块链网络的交易系统架构图。如图 1 所示，整个交易系统可包括区块链网络 20 和客户端 10。在区块链网络 20 内包括多个验证节点。可基于不同业务场景、群体或业务垂直领域对系统中的验证节点进行分区。例如，在每个验证节点的公钥地址前可具有相应分区的分区标识。每个分区包括若干的验证节点，用于对交易进行 Query（请求）或 Commit（确认）过程。

图 2 也示出了一种基于区块链网络的交易系统架构图，其中区块链网络包括多个验证节点，其中的一部分被划分为 Query 分区，其中的又一部分被划分为 Commit 分区。需要指出的是，该划分可基于业务场景、群体或业务垂直领域而进行。在一个示例中，在每个验证节点的公钥地址前可具有相应分区的分区标识。每个分区包括若干的验证节点，用于对交易进行 Query（请求）或 Commit（确认）过程。

与图 1 不同，图 2 进一步示出了网关和系统路由装置。在图 2 的示例中，用户通过客户端提交的交易申请会经由网关、系统路由装置发送至区块链网络内的各个分区。

在一个实施例中，客户端负责接收用户的交易请求（请求包括

节点动态加入和交易请求），对交易输入、输出部分连同进行组包形成交易哈希值发送给网关。网关负责将交易哈希值进行解析，形成一个多输入、多输出的形式，并将结果发送至系统路由装置。系统路由装置根据网关解析的结果，将每一笔输入、输出发往其所对应的 Query 及 Commit 分区进行验证，其中包括防双花验证、交易合法性验证两个部分，交易验证成功后对整笔交易进行记录。

图 3 示意示出了本发明的一个实施例的基于区块链网络的交易方法 3000。区块链网络可参照图 1 或 2 中描述的区块链网络 20，其中包括多个验证节点，该多个验证节点中的第一部分被划分为第一分区，该多个验证节点中的第二部分被划分为第二分区，划分可基于业务场景、群体或业务垂直领域而进行。

在步骤 310 中，第一分区内的验证节点对来自客户端的第一交易请求进行验证。

在步骤 320 中，在验证通过后，第一分区内的验证节点对第一交易请求进行签名，并返回客户端。

在步骤 330 中，第二分区内的验证节点对来自客户端的第二交易请求进行验证。

在步骤 340 中，在验证通过后，第二分区内的验证节点将交易信息记入账本。

有必要指出的是，在上述交易方法 3000 中，第一交易请求包括交易内容，以及第二交易请求包括交易内容和客户端收集的第一分区内的验证节点的签名。

上述方法以多分区概念为基础，通过分区局部共识来减少因全网共识产生的通讯开销，从而提高系统处理性能。

参考图 4，它具体示出了根据本发明的一个实施例的交易请求处理过程。如图 4 所示，其可包括四大部分：交易解析、Query 分区防双花验证、客户端执行交易以及验证交易。

在交易解析过程中，例如由网关将交易哈希值进行解析，形成一个多输入、多输出的形式，并将结果发送至系统路由装置。系统路由装置随后根据网关分析的结果，通过交易中的每一个输入项，寻找其

所属的 Query 分区，并发送交易。上述交易解析过程在一个实施例中也可由客户端单独实现。

在一个实施例中，交易被解析成 N 输入和 N 输出，所述输入、输出均为元组，分别表示为 ('InputTx', [' keyid_in', 'pos', 'value_in'])、('OutputTx', ['keyid_out', 'value_out'])，其中 keyid_in 为当笔输入对应的交易地址，pos 指该交易地址所属分区标识，value_in 为当笔输入所对应的价值，keyid_out 为所述接收方的交易地址，value_out 为支付给该接收方的价值。

在 Query 分区防双花验证过程中，分区内各个验证节点对交易进行验证，包括防双花、交易合法性等，在验证通过后对交易签名。在一个实施例中，通过解析出的 N 项输入，将每一笔输入根据其所属 pos 标识，发送至交易地址所属 Query 分区。各验证节点会对该笔交易的 input 进行防双花确认，通过确认后以 Query(node, tx, input, timestamp) 的形式记入日志，然后对交易信息进行签名 ($\sigma \xleftarrow{\$} Sig.sig(\mathrm{pk}, (\mathrm{tx}, \mathrm{input}, \mathrm{node}, \mathrm{h}, \mathrm{n}))$)，并返回给客户端。

在客户端执行交易过程中，客户端收集 Query 分区内验证节点发来的签名，将其与交易打包发送至 Commit 分区。在一个实施例中，客户端收集 Query 分区内 Node1、Node2、Node3 发送来的数字签名 σ，根据每一项输出所属 pos 标识，将收集的签名连同该交易一起发送至 Commit 验证分区的节点 Node4、Node5、Node6。

在验证交易过程中，Commit 分区对交易信息进行验证，着重判断该交易是否得到 Query 分区半数以上节点的签名，在验证通过后，记入账本。在一个实施例中，验证节点对用户发送来的信息进行验证，验证通过后会以 Commit(node, tx, signs, timestamp)的形式记入日志，同时将该交易 tx 记录至账本中。当同一片区内大于一半的记账节点记录该交易后，视为达成共识，该笔交易将不可篡改，并会将交易成功信息发送给用户。

需要强调的是，在本发明的上下文中，日志与账本是两种不同的概念，日志的作用是为日志哈希链服务，主要用于审计验证节点行为，而账本是指系统内验证节点保证一致性的交易账本，用于记录交易内

容。

在本发明的一个实施例中，上述交易方法包含了对验证节点行为进行审计的策略，该审计策略的实施需依托节点自身的日志哈希链，具体实施方案如下：

系统中所有验证节点均具有自身的日志哈希链，该日志中的内容包括“Query（请求）”、“Commit（确认）”两种。“Query（请求）”是指节点接收到交易请求后，针对交易内容中用户的数字签名、输入是否双花进行验证，验证通过后以 Query(node, tx, input, timestamp)的形式记入日志，node 指当前验证节点序号，tx 为交易哈希值，input 为验证节点验证通过的交易输入，timestamp 为当前时间戳。当前日志哈希链的链头值会随着这条 Query 记录的加入而发生改变，h_n=H(Query‖h_(n-1))，式中 h_n 指第 n 条记录后的哈希链头值，Query 指当前记录，h_(n-1)指日志中前 n-1 条的哈希链头值。当前日志的哈希链头值通过签名($\sigma \xleftarrow{\$} Sig.sig(pk,(tx,input,node,h,n))$)的形式传输给交易 Commit（确认）验证节点，式中 σ 为数字签名，pk 为发送信息节点的公钥，tx 为交易哈希值，input 为节点验证通过的交易输入，node 指节点序号，h 为当前链头值，n 为对应的记录序列号。交易“Commit（确认）”节点收到前述各节点发来的签名后，会对这些签名进行验证（包括签名中所包含的输入、节点序号、日志链头值等），验证成功后会以 Commit(node, tx, signs, timestamp)的形式记入日志，node 指当前节点序号，tx 为交易哈希值，signs 为节点收到的所有签名，timestamp 为当前时间戳。当前日志哈希链的链头值会随着这条 Commit 记录的加入而发生改变，h_m=H(Commit‖h_(m-1))，式中 h_m 指第 m 条记录后的哈希链头值，Commit 指当前记录，h_(m-1)指日志中前 m-1 条的哈希链头值。

以此类推，即在整个区块链系统中，所有节点针对一笔交易的 Query 和 Commit 行为将不仅仅由自身记录，而是会广播到系统内的所有节点，并同时记录在这些节点的日志中，形成了系统内节点间即时交叉验证的网络，当某一节点想要去篡改记录或者不作为时，该节点的日志会将其作弊行为暴露，保证整个系统的正常运行。

如图 4 所示，每一个节点都具有其自身的日志哈希链，记录其在共识协议中的行为，包括 Query（请求）和 Commit（确认）行为。例如，当客户端提交一笔新的交易 tx 至节点 1-3 时，在防双花验证通过后会以 Query 的形式记录在日志中，并将当前的链头值（h_n）以签名的形式传送给客户端；客户端收集到超过半数的签名（signs，签名中包含每一个验证者当前的链头值作为见证）后，将这些签名连同交易发送至节点 4-6 进行交易验证；交易验证通过后，节点 4-6 会将客户端发来的所有 signs 以 Commit 的形式记录在日志中，并生成一个新的链头值（h_m）。

引入日志哈希链后，针对同一笔交易过程中“请求”、“确认”两个阶段行为的互相记录和验证，使得任何节点作弊及不作为行为均会在全网可见的日志中被发现。

此外，本发明的基于区块链网络的交易方法可通过代码的方式进行实现。该代码可存储在各种计算机存储介质（包括但不限于磁盘、磁带、光盘、硬盘、U 盘、SD 卡以及内存条等）上。

综上，本发明的技术方案提出基于区块链网络节点分区的交易方法及系统，以分区的方式提高系统的交易处理能力。此外，区块链系统网络内节点的行为可通过对日志数据进行系统分析处理，形成节点间相互审计，形成各节点行为的互相见证（或交叉验证）。

以上例子主要说明了基于区块链网络中网络节点分区的方案。尽管只对其中一些本发明的具体实施方式进行了描述，但是本领域普通技术人员应当了解，本发明可以在不偏离其主旨与范围内以许多其他的形式实施。因此，所展示的例子与实施方式被视为示意性的而非限制性的，在不脱离如所附各权利要求所定义的本发明精神及范围的情况下，本发明可能涵盖各种的修改与替换。

权 利 要 求 书

1. 一种区块链网络，其特征在于，所述网络包括：

多个验证节点，所述多个验证节点中的第一部分被划分为第一分区，所述多个验证节点中的第二部分被划分为第二分区，

其中，所述划分基于业务场景、群体或业务垂直领域而进行，

所述第一分区内的验证节点配置成对来自客户端的第一交易请求进行验证，并在验证通过后对所述第一交易请求进行签名，并返回所述客户端；以及

所述第二分区内的验证节点配置成对来自所述客户端的第二交易请求进行验证，并在验证通过后记入账本，其中所述第一交易请求包括交易内容，以及所述第二交易请求包括所述交易内容和所述客户端收集的所述第一分区内的验证节点的签名。

2. 如权利要求 1 所述的区块链网络，其中，所述第一分区内的验证节点配置成在收到所述第一交易请求后，针对所述交易内容中的用户的数字签名、输入是否双花进行验证。

3. 如权利要求 1 所述的区块链网络，其中，所述第二分区内的验证节点配置成判断所述第二交易请求中的交易是否得到所述第一分区内半数以上的验证节点的签名。

4. 如权利要求 2 所述的区块链网络，其中，所述第一分区内的验证节点是请求节点，其配置成在验证通过后，以 Query(node, tx, input, timestamp)的形式记入日志，其中 node 为当前验证节点序号，tx 为交易哈希值，input 为验证节点验证通过的交易输入，timestamp 为当前时间戳。

5. 如权利要求 3 所述的区块链网络，其中，所述第二分区内的验证节点为确认节点，其配置成在验证通过后，以 Commit (node, tx, signs, timestamp)的形式记入日志，其中 node 为当前验证节点序号，tx 为交易哈希值，signs 为验证节点收到的所有签名，timestamp 为当前时间戳。

6. 如权利要求 1 所述的区块链网络，其中，所述多个验证节点

中的每一个具有其自身的日志哈希链，用于记录其在共识协议中的请求和/或确认行为。

7. 一种基于区块链网络的交易方法，其特征在于，所述区块链网络包括多个验证节点，所述多个验证节点中的第一部分被划分为第一分区，所述多个验证节点中的第二部分被划分为第二分区，所述划分基于业务场景、群体或业务垂直领域而进行，所述方法包括：

所述第一分区内的验证节点对来自客户端的第一交易请求进行验证；

在验证通过后，所述第一分区内的验证节点对所述第一交易请求进行签名，并返回所述客户端；

所述第二分区内的验证节点对来自所述客户端的第二交易请求进行验证；以及

在验证通过后，所述第二分区内的验证节点将交易信息记入账本，其中所述第一交易请求包括交易内容，以及所述第二交易请求包括所述交易内容和所述客户端收集的所述第一分区内的验证节点的签名。

8. 如权利要求 7 所述的方法，其中，所述第一分区内的验证节点对来自客户端的第一交易请求进行验证包括：

在收到所述第一交易请求后，所述第一分区内的验证节点针对所述交易内容中的用户的数字签名、输入是否双花进行验证。

9. 如权利要求 7 所述的方法，其中，所述第二分区内的验证节点对来自所述客户端的第二交易请求进行验证包括：

所述第二分区内的验证节点判断所述第二交易请求中的交易是否得到所述第一分区内半数以上的验证节点的签名。

10. 如权利要求 8 所述的方法，其中，在验证通过后，所述第一分区内的验证节点对所述第一交易请求进行签名，并返回所述客户端包括：

所述第一分区内的验证节点在验证通过后，以 Query(node, tx, input, timestamp)的形式记入日志，其中 node 为当前验证节点序号，tx 为交易哈希值，input 为验证节点验证通过的交易输入，timestamp

为当前时间戳。

11. 如权利要求 9 所述的方法，其中，在验证通过后，所述第二分区内的验证节点将交易信息记入账本包括：

所述第二分区内的验证节点在验证通过后，以 Commit (node, tx, signs, timestamp)的形式记入日志，其中 node 为当前验证节点序号，tx 为交易哈希值，signs 为验证节点收到的所有签名，timestamp 为当前时间戳。

12. 如权利要求 7 所述的方法，其中，所述多个验证节点中的每一个具有其自身的日志哈希链，用于记录其在共识协议中的请求和/或确认行为。

13. 一种计算机存储介质，其特征在于，所述介质包括指令，所述指令在被执行时，实现如权利要求 7 至 12 中任一项所述的方法。

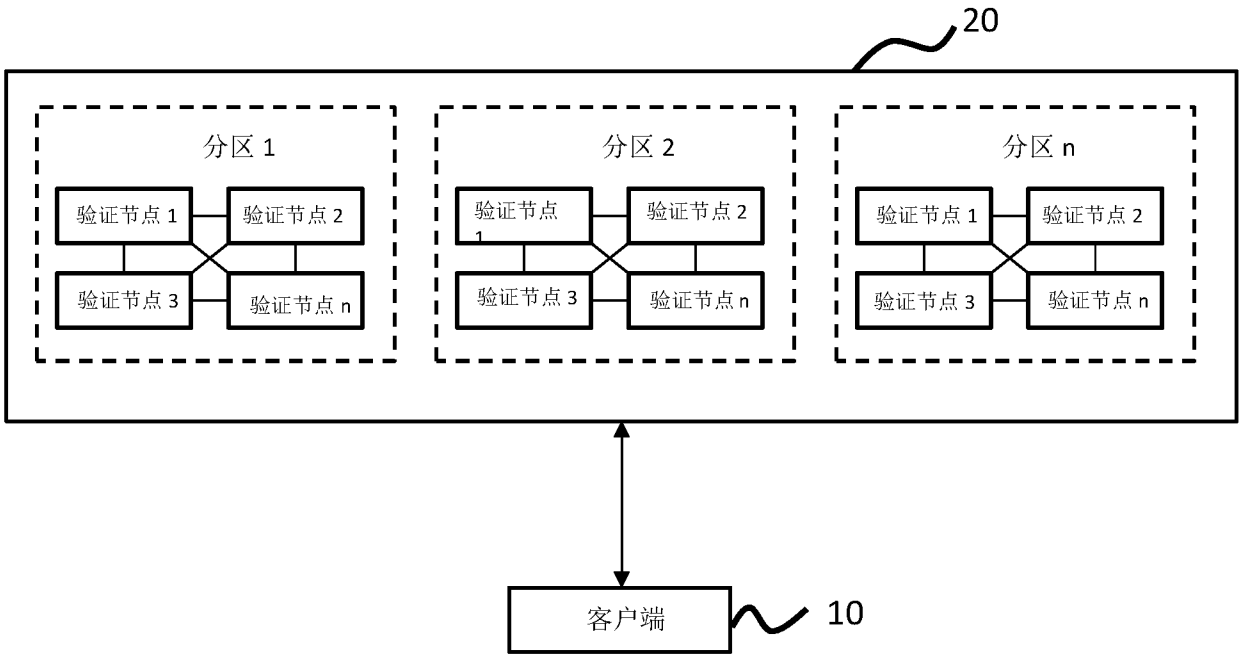
20
分区 1
验证节点 1
验证节点 2
验证节点 3
验证节点 n
分区 2
验证节点 1
验证节点 2
验证节点 3
验证节点 n
分区 n
验证节点 1
验证节点 2
验证节点 3
验证节点 n
客户端
10

图 1

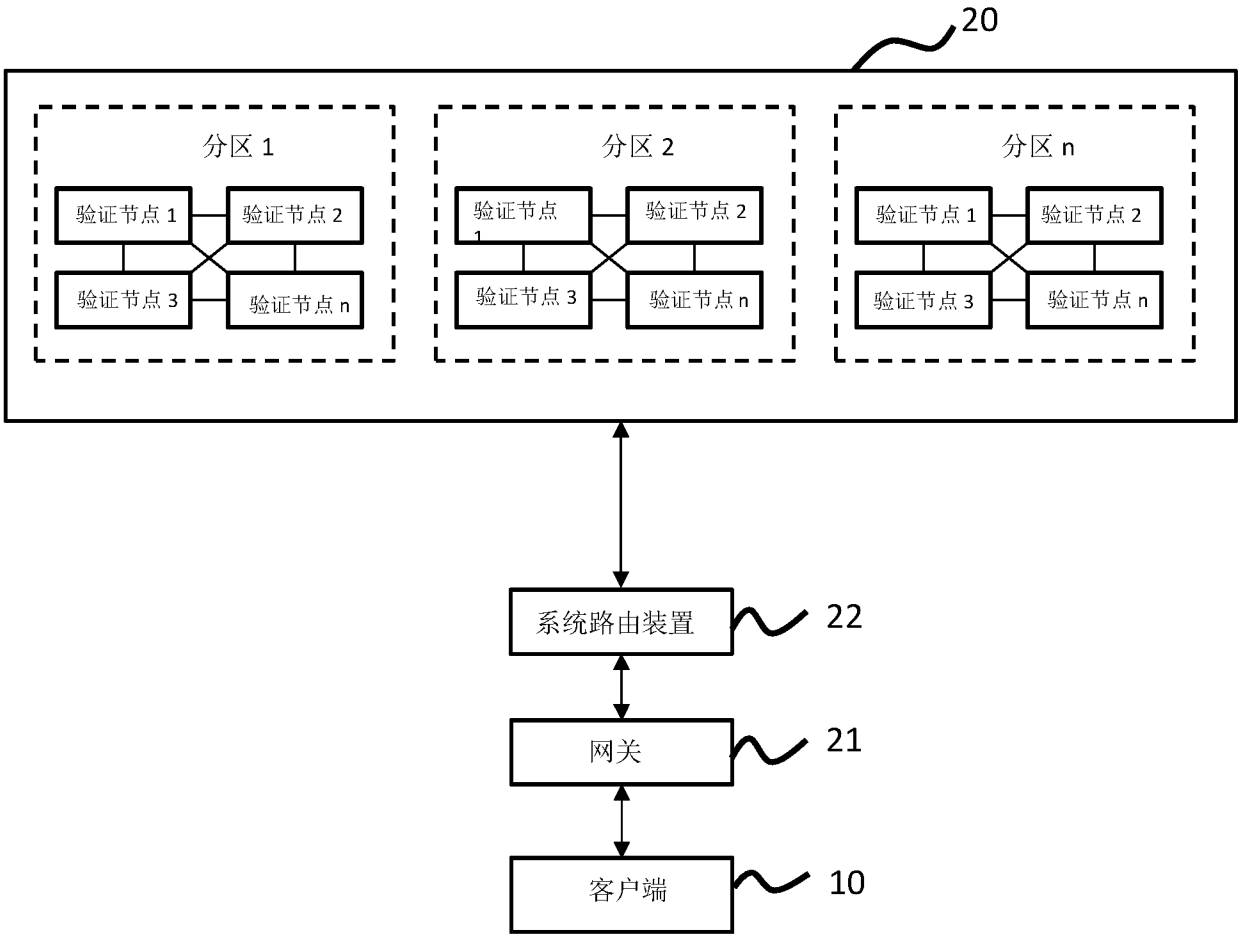
20
分区 1
验证节点 1
验证节点 2
验证节点 3
验证节点 n
分区 2
验证节点 1
验证节点 2
验证节点 3
验证节点 n
分区 n
验证节点 1
验证节点 2
验证节点 3
验证节点 n
系统路由装置
22
网关
21
客户端
10

图 2

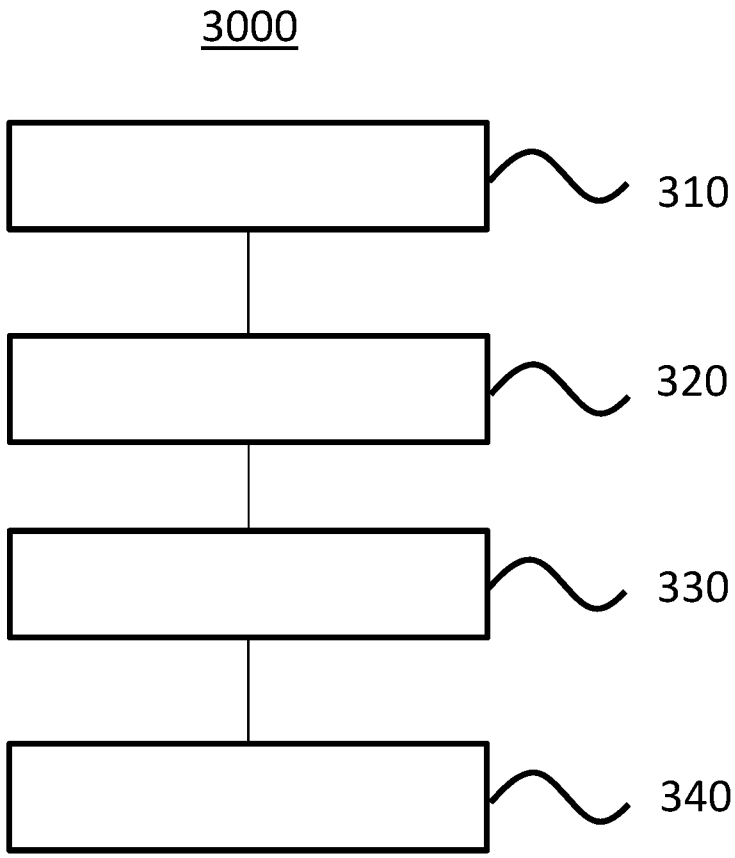

图 3

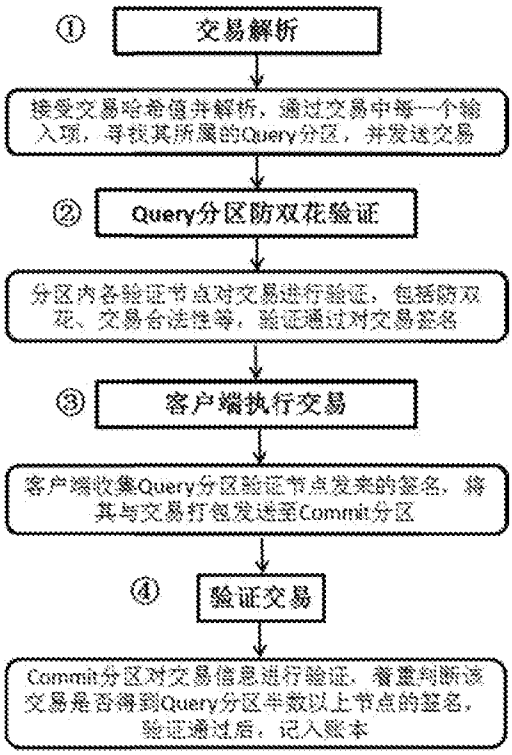
①
交易解析
接受交易哈希值并解析，通过交易中每一个输入项，寻找其所属的Query分区，并发送交易
②
Query分区防双花验证
分区内各验证节点对交易进行验证，包括防双花、交易合法性等，验证通过对交易签名
③
客户端执行交易
客户端收集Query分区验证节点发来的签名，将其与交易打包发送至Commit分区
④
验证交易
Commit分区对交易信息进行验证，重点判断该交易是否得到Query分区半数以上节点的签名，验证通过后，记入账本

图 4

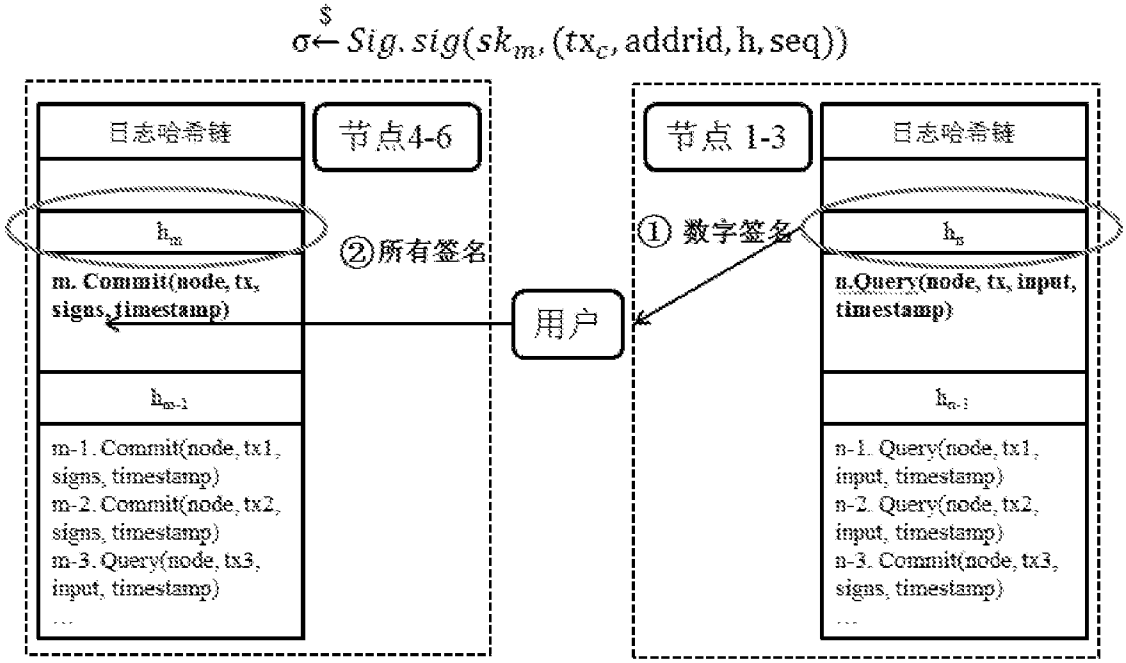
$\sigma \xleftarrow{\$} Sig.sig(sk_m, (tx_c, addrid, h, seq))$
日志哈希链
节点4-6
h_m
m. Commit(node, tx, signs, timestamp)
h_{m-1}
m-1. Commit(node, tx1, signs, timestamp)
m-2. Commit(node, tx2, signs, timestamp)
m-3. Query(node, tx3, input, timestamp)
...
②所有签名
用户
节点 1-3
日志哈希链
① 数字签名
h_n
n.Query(node, tx, input, timestamp)
h_{n-1}
n-1. Query(node, tx1, input, timestamp)
n-2. Query(node, tx2, input, timestamp)
n-3. Commit(node, tx3, signs, timestamp)
...

图 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2018/109246

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32(2006.01)i; G06Q 20/40(2012.01)n

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F; G06Q; H04L

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

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

CNPAT, CNKI, WPI, EPODOC, GOOGLE: 区块链, 联盟链, 比特币, 分布式, 账本, 记账, 账务, 账目, 划分, 分区, 分层, 分级, 分为, 分支, 分组, 拆分, 交易, 业务, 买卖, 签名, 验证, 认证, 鉴权, 登记, 记入, 写入, 记录, 存储, 储存, 保存, 查询, 问询, 询问, 确认, blockchain, distribut+, ledger+, account?, BTC, bitcoin, divid+, separat+, split+, group+, cluster+, transaction, trad+, service, business, sign+, authen+, author+, validat+, writ+, stor+, query, commit+

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
PX	CN 108023729 A (CHINA UNIONPAY CO., LTD.) 11 May 2018 (2018-05-11) claims 1-13	1-13
X	CN 107196900 A (ALIBABA GROUP HOLDING LIMITED) 22 September 2017 (2017-09-22) description, paragraphs [0007]-[0029] and [0050]	1-3, 6-9, 12-13
A	CN 106656974 A (JIANGSU PAY EGIS TECHNOLOGY CO., LTD.) 10 May 2017 (2017-05-10) entire document	1-13
A	WO 2017175073 A1 (VCHAIN TECHNOLOGY LIMITED) 12 October 2017 (2017-10-12) entire document	1-13

☐ Further documents are listed in the continuation of Box C. ☑ See patent family annex.

* Special categories of cited documents:

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
06 December 2018	**29 December 2018**

Name and mailing address of the ISA/CN	Authorized officer
State Intellectual Property Office of the P. R. China **No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing** **100088** **China**	
Facsimile No. **(86-10)62019451**	Telephone No.

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2018/109246

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
CN	108023729	A	11 May 2018	None			
CN	107196900	A	22 September 2017	WO	2018175540	A1	27 September 2018
				US	2018276668	A1	27 September 2018
CN	106656974	A	10 May 2017	None			
WO	2017175073	A1	12 October 2017	US	2017286717	A1	05 October 2017

国际检索报告

国际申请号 PCT/CN2018/109246

A. 主题的分类

H04L 9/32(2006.01)i; G06Q 20/40(2012.01)n

按照国际专利分类(IPC)或者同时按照国家分类和IPC两种分类

B. 检索领域

检索的最低限度文献(标明分类系统和分类号)

G06F; G06Q; H04L

包含在检索领域中的除最低限度文献以外的检索文献

在国际检索时查阅的电子数据库(数据库的名称，和使用的检索词（如使用）)

CNPAT,CNKI,WPI,EPODOC,GOOGLE: 区块链，联盟链，比特币，分布式，账本，记账，账务，账目，划分，分区，分层，分级，分为，分支，分组，拆分，交易，业务，买卖，签名，验证，认证，鉴权，登记，记入，写入，记录，存储，储存，保存，查询，问询，询问，确认， blockchain, distribut+, ledger+, account?, BTC, bitcoin, divid+, separat+, split+, group+, cluster+, transaction, trad+, service, business, sign+, authen+, author+, validat+, writ+, stor+, query, commit+

C. 相关文件

类 型*	引用文件，必要时，指明相关段落	相关的权利要求
PX	CN 108023729 A (中国银联股份有限公司) 2018年 5月 11日 (2018-05-11) 权利要求1-13	1-13
X	CN 107196900 A (阿里巴巴集团控股有限公司) 2017年 9月 22日 (2017-09-22) 说明书第[0007]-[0029]、[0050]段	1-3、6-9、12-13
A	CN 106656974 A (江苏通付盾科技有限公司) 2017年 5月 10日 (2017-05-10) 全文	1-13
A	WO 2017175073 A1 (VCHAIN TECHNOLOGY LIMITED) 2017年 10月 12日 (2017-10-12) 全文	1-13

☐ 其余文件在C栏的续页中列出。

☑ 见同族专利附件。

* 引用文件的具体类型：

"A" 认为不特别相关的表示了现有技术一般状态的文件

"E" 在国际申请日的当天或之后公布的在先申请或专利

"L" 可能对优先权要求构成怀疑的文件，或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件（如具体说明的）

"O" 涉及口头公开、使用、展览或其他方式公开的文件

"P" 公布日先于国际申请日但迟于所要求的优先权日的文件

"T" 在申请日或优先权日之后公布，与申请不相抵触，但为了理解发明之理论或原理的在后文件

"X" 特别相关的文件，单独考虑该文件，认定要求保护的发明不是新颖的或不具有创造性

"Y" 特别相关的文件，当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时，要求保护的发明不具有创造性

"&" 同族专利的文件

国际检索实际完成的日期	国际检索报告邮寄日期
2018年 12月 6日	2018年 12月 29日
ISA/CN的名称和邮寄地址 中国国家知识产权局(ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10)62019451	受权官员 张枫 电话号码 86-(10)-53961628

国际检索报告
关于同族专利的信息

国际申请号
PCT/CN2018/109246

检索报告引用的专利文件			公布日（年/月/日）	同族专利			公布日（年/月/日）
CN	108023729	A	2018年 5月 11日		无		
CN	107196900	A	2017年 9月 22日	WO	2018175540	A1	2018年 9月 27日
				US	2018276668	A1	2018年 9月 27日
CN	106656974	A	2017年 5月 10日		无		
WO	2017175073	A1	2017年 10月 12日	US	2017286717	A1	2017年 10月 5日