(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 117716366 A
(43)申请公布日 2024.03.15

(21)申请号 202280052498.9

(22)申请日 2022.07.22

(30)优先权数据
63/228,772 2021.08.03 US

(85)PCT国际申请进入国家阶段日
2024.01.26

(86)PCT国际申请的申请数据
PCT/JP2022/028475 2022.07.22

(87)PCT国际申请的公布数据
WO2023/013446 JA 2023.02.09

(71)申请人 松下电器(美国)知识产权公司
地址 美国加利福尼亚

(72)发明人 中坂绫香 海上勇二 山本格也 芳贺智之

(74)专利代理机构 永新专利商标代理有限公司 72002
专利代理师 高迪

(51)Int.Cl.
G06F 21/64(2006.01)

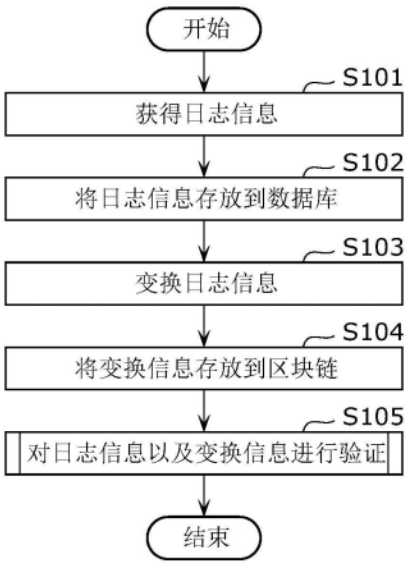
权利要求书2页 说明书14页 附图7页

(54)发明名称

验证方法、服务器、以及程序

(57)摘要

一种验证方法,在该验证方法中,(S101)通过设备进行工作,来从设备依次地获得在设备生成的多个日志信息;(S102)将多个日志信息依次地存放到存储装置;并且(S104)将多个日志信息以规定的变换分别进行变换,并将变换后的多个变换信息依次地存放到区块链;(S105)根据多个日志信息中的验证对象的对象日志信息、以及多个变换信息中的对象日志信息所对应的对象变换信息,以规定的频度来执行对象日志信息以及对象变换信息的至少其中一方是否被篡改的验证,规定的频度以如下的方式来决定,即在对象变换信息被存放到区块链的时刻越接近进行验证的当前时刻,就决定越高的频度。



CN 117716366 A

1.一种验证方法,在该验证方法中,

通过设备进行工作,从而从所述设备依次获得在所述设备生成的多个日志信息,

将所述多个日志信息依次地存放到存储装置,并且将所述多个日志信息的每一个以规定的变换来进行变换,将通过变换而得到的多个变换信息依次地存放到区块链,

根据所述多个日志信息中的验证对象的对象日志信息、以及所述多个变换信息中的与所述对象日志信息对应的对象变换信息,以规定的频度来执行所述对象日志信息以及所述对象变换信息的至少其中一方是否被篡改的验证,

所述规定的频度以如下的方式来决定,即所述对象变换信息被存放到所述区块链的时刻越接近进行所述验证时的当前时刻,就决定越高的频度。

2.如权利要求1所述的验证方法,

所述规定的频度以如下的方式来决定,即包括所述对象变换信息的第1区块在所述区块链中的位置离最后连结到所述区块链的第2区块越近,就决定越高的频度。

3.如权利要求1所述的验证方法,

所述多个日志信息的每一个被分类为,按日志信息的属性而预先决定的多个级别的重要度,

所述规定的频度进一步以所述重要度越高,则频度就越高的方式来决定。

4.如权利要求1所述的验证方法,

所述多个日志信息的每一个被分类为,按日志信息的属性而预先决定的多个级别的重要度,

所述规定的频度以如下的方式来决定,即包括所述对象变换信息的第1区块在所述区块链中的位置离最后连结到所述区块链的第2区块越近,就决定越高的频度,并且所述重要度越高,就决定越高的频度。

5.如权利要求4所述的验证方法,

所述规定的频度由表格来决定,

所述表格由分别与多个组对应的多个频度来表现,所述多个组是以区块链中的相对位置来分类的多个范围与重要度的级别的配对。

6.如权利要求5所述的验证方法,

在所述区块链中存放有如下的智能合约,该智能合约是在包括用于更新所述表格的交易数据的区块被存放到所述区块链时,用来执行更新所述表格中设定的所述多个频度的更新处理的智能合约。

7.如权利要求1至6的任一项所述的验证方法,

在所述验证中,通过将所述对象日志信息以所述规定的变换来进行变换,从而生成验证用的变换信息,对所述验证用的变换信息与所述区块链中存放的所述对象变换信息进行比较,若比较的结果为一致,则判断为所述对象日志信息以及所述对象变换信息没有被篡改,若比较的结果为不一致,则判断为所述对象日志信息以及所述对象变换信息的至少其中一方被篡改。

8.如权利要求7所述的验证方法,

所述规定的变换是将第1值变换为与所述第1值配对的唯一的第2值的具有再现性的方法,并且所述规定的变换是不能从所述第2值变换为所述第1值的不可逆的变换。

9.一种服务器,具备处理器和存储器,

所述处理器利用所述存储器,

从设备依次地获得所述设备进行工作而生成的多个日志信息,

将所述多个日志信息依次地存放到存储装置,并且将所述多个日志信息的每一个以规定的变换来进行变换,将通过变换而得到的多个变换信息依次地存放到区块链,

根据所述多个日志信息中的验证对象的对象日志信息、以及所述多个变换信息中的与所述对象日志信息对应的对象变换信息,以规定的频度来执行所述对象日志信息以及所述对象变换信息的至少其中一方是否被篡改的验证,

所述规定的频度以如下的方式来决定,即所述对象变换信息被存放到所述区块链的时刻越接近当前时刻,就决定越高的频度。

10.一种程序,用于使计算机执行如下的工作:

从设备依次地获得所述设备进行工作而生成的多个日志信息,

将所述多个日志信息依次地存放到存储装置,并且将所述多个日志信息的每一个以规定的变换来进行变换,将通过变换而得到的多个变换信息依次地存放到区块链,

根据所述多个日志信息中的验证对象的对象日志信息、以及所述多个变换信息中的与所述对象日志信息对应的对象变换信息,以规定的频度来执行所述对象日志信息以及所述对象变换信息的至少其中一方是否被篡改的验证,

所述规定的频度以如下的方式来决定,即所述对象变换信息被存放到所述区块链的时刻越接近进行所述验证时的当前时刻,就决定越高的频度。

验证方法、服务器、以及程序

技术领域

[0001] 本公开涉及验证方法、服务器、以及程序。

背景技术

[0002] 在非专利文献1中公开了一种以区块链和数据外套(Data Jacket)为基础的技术，所述数据外套(Data Jacket)是使数据的内容隐匿来使数据所持有的价值共享的一种方法。

[0003] 现有技术文献

[0004] 非专利文献

[0005] 非专利文献1池田栄次他:「ブロックチェーン×データジャケット」によるデータ流通・利活用社会への加速:IEICE Technical Report.AI2017-25(2018)(池田荣次等著:基于“区块链×数据外套”的数据流通以及社会灵活运用的加速)

发明内容

[0006] 本公开的目的在于提供一种能够对篡改进行轻量级检测的验证方法等。

[0007] 在本公开的一个方式所涉及的验证方法中，通过设备进行工作，从而从所述设备依次获得在所述设备生成的多个日志信息，将所述多个日志信息依次地存放到存储装置，并且将所述多个日志信息的每一个以规定的变换来进行变换，将通过变换而得到的多个变换信息依次地存放到区块链，根据所述多个日志信息中的验证对象的对象日志信息、以及所述多个变换信息中的与所述对象日志信息对应的对象变换信息，以规定的频度来执行所述对象日志信息以及所述对象变换信息的至少其中一方是否被篡改的验证，所述规定的频度以如下的方式来决定，即所述对象变换信息被存放到所述区块链的时刻越接近进行所述验证时的当前时刻，就决定越高的频度。

[0008] 另外，这些概括性的或具体的方式可以由系统、装置、集成电路、计算机程序或计算机可读的CD-ROM等记录介质来实现，也可以通过系统、装置、集成电路、计算机程序以及记录介质的任意组合来实现。

[0009] 通过本公开，能够对篡改进行轻量级检测。

附图说明

[0010] 图1示出了实施方式所涉及的数据流通系统的构成的一个例子。

[0011] 图2示出了实施方式所涉及的信息终端的构成的一个例子。

[0012] 图3示出了实施方式所涉及的服务器的构成的一个例子。

[0013] 图4示出了区块链中的区块的位置。

[0014] 图5示出了决定了规定的频度的表格的一个例子。

[0015] 图6是示出实施方式所涉及的数据流通系统的工作的一个例子的流程图。

[0016] 图7是示出通过实施方式所涉及的数据流通系统进行的验证处理的一个例子的流

程图。

[0017] 图8是用于说明数据流通系统的工作的具体例子的图。

[0018] 图9是用于说明数据流通系统的工作的具体例子的图。

具体实施方式

[0019] (得到本公开的经过)

[0020] 近些年,针对使医疗保健等个人数据在企业间流通的系统的社会需求不断地增高,因此作为提高该系统的抗篡改性的方法,区块链技术受到关注。通过将从数据流通系统进行数据下载等各种操作日志记录到数据库和区块链这双方,从而可以使篡改变得困难。在此考虑到的篡改检测是通过对记录到数据库和区块链这双方的操作日志进行比较来进行验证,若对被记录的所有的操作日志高频度地进行验证,则该验证所需要的计算量就会随着时间的经过而增大,因此长期地运用将成为课题。于是,本发明人员在系统的操作日志随着时间的经过而增大这种条件下发现了如下的验证方法,具体是通过按照操作日志的类别和区块链的时间序列数据结构来高效地选择验证对象日志,从而能够对篡改进行轻量级检测。

[0021] 在本公开的第1个方式所涉及的验证方法中,通过设备进行工作,从而从所述设备依次获得在所述设备生成的多个日志信息,将所述多个日志信息依次地存放到存储装置,并且将所述多个日志信息的每一个以规定的变换来进行变换,将通过变换而得到的多个变换信息依次地存放到区块链,根据所述多个日志信息中的验证对象的对象日志信息、以及所述多个变换信息中的与所述对象日志信息对应的对象变换信息,以规定的频度来执行所述对象日志信息以及所述对象变换信息的至少其中一方是否被篡改的验证,所述规定的频度以如下的方式来决定,即所述对象变换信息被存放到所述区块链的时刻越接近进行所述验证时的当前时刻,就决定越高的频度。

[0022] 据此,对象变换信息被存放到区块链的时刻越接近进行验证的当前时刻,就以越高的频度来执行对该对象变换信息的验证,因此能够使针对篡改的风险又低又旧的对象变换信息的验证的频度变低。因此,能够按照篡改的风险来执行验证,从而能够在不使篡改的风险增大的状态下,来减少验证的次数。因此,能够执行轻量级验证。

[0023] 在本公开的第2个方式所涉及的验证方法中,以第1个方式所涉及的验证方法为前提,所述规定的频度以如下的方式来决定,即包括所述对象变换信息的第1区块在所述区块链中的位置离最后连结到所述区块链的第2区块越近,就决定越高的频度。

[0024] 因此,越是对象变换信息被存放到区块链的时刻接近进行验证的当前时刻的区块中的变换信息,就以越高的频度被执行验证,因此能够使针对篡改的风险又低又旧的对象变换信息的验证的频度变低。

[0025] 在本公开的第3个方式所涉及的验证方法中,以第1个方式所涉及的验证方法为前提,所述多个日志信息的每一个被分类为,按日志信息的属性而预先决定的多个级别的重要度,所述规定的频度进一步以所述重要度越高,则频度就越高的方式来决定。

[0026] 据此,由于能够按日志信息的属性,来设定给规定的频度造成影响的重要度,因此,越是由于篡改而风险影响程度高的日志信息,就能够以越高的频度被执行验证。

[0027] 在本公开的第4个方式所涉及的验证方法中,以第1个方式所涉及的验证方法为前

提,所述多个日志信息的每一个被分类为,按日志信息的属性而预先决定的多个级别的重要度,所述规定的频度以如下的方式来决定,即包括所述对象变换信息的第1区块在所述区块链中的位置离最后连结到所述区块链的第2区块越近,就决定越高的频度,并且所述重要度越高,就决定越高的频度。

[0028] 因此,越是对象变换信息被存放到区块链的时刻接近进行验证的当前时刻的区块中的变换信息,就以越高的频度被执行验证,因此能够使针对篡改的风险又低又旧的对象变换信息的验证的频度变低。并且,由于还能够按日志信息的属性,来设定给规定的频度造成影响的重要度,因此,越是由于篡改而风险影响程度高的日志信息,就能够以越高的频度被执行验证。

[0029] 在本公开的第5个方式所涉及的验证方法中,以第4个方式所涉及的验证方法为前提,所述规定的频度由表格来决定,所述表格由分别与多个组对应的多个频度来表现,所述多个组是以区块链中的相对位置来分类的多个范围与重要度的级别的配对。

[0030] 因此,能够通过参照表格来决定规定的频度。

[0031] 在本公开的第6个方式所涉及的验证方法中,以第5个方式所涉及的验证方法为前提,在所述区块链中存放有如下的智能合约,该智能合约是在包括用于更新所述表格的交易数据的区块被存放到所述区块链时,用来执行更新所述表格中设定的所述多个频度的更新处理的智能合约。

[0032] 据此,能够将交易数据被存放到区块链作为契机,利用智能合约来自动地更新表格。并且,由于能够通过更新表格来对规定的频度进行更新,因此能够减轻对规定的频度进行更新的处理所需要的处理负荷。

[0033] 在本公开的第7个方式所涉及的验证方法中,以第1个方式到第6个方式所涉及的验证方法为前提,在所述验证中,通过将所述对象日志信息以所述规定的变换来进行变换,从而生成验证用的变换信息,对所述验证用的变换信息与所述区块链中存放的所述对象变换信息进行比较,若比较的结果为一致,则判断为所述对象日志信息以及所述对象变换信息没有被篡改,若比较的结果为不一致,则判断为所述对象日志信息以及所述对象变换信息的至少其中一方被篡改。

[0034] 在本公开的第8个方式所涉及的验证方法中,以第7个方式所涉及的验证方法为前提,所述规定的变换是将第1值变换为与所述第1值配对的唯一的第2值的具有再现性的方法,并且所述规定的变换是不能从所述第2值变换为所述第1值的不可逆的变换。

[0035] 因此,能够提高对数据库中存放的数据进行验证的、被存放在开放的区块链的数据的匿名性。

[0036] 本公开的第9个方式所涉及的服务器具备处理器和存储器,所述处理器利用所述存储器,从设备依次地获得所述设备进行工作而生成的多个日志信息,将所述多个日志信息依次地存放到存储装置,并且将所述多个日志信息的每一个以规定的变换来进行变换,将通过变换而得到的多个变换信息依次地存放到区块链,根据所述多个日志信息中的验证对象的对象日志信息、以及所述多个变换信息中的与所述对象日志信息对应的对象变换信息,以规定的频度来执行所述对象日志信息以及所述对象变换信息的至少其中一方是否被篡改的验证,所述规定的频度以如下的方式来决定,即所述对象变换信息被存放到所述区块链的时刻越接近当前时刻,就决定越高的频度。

[0037] 据此,越是对象变换信息被存放到区块链的时刻接近进行验证的当前时刻的区块中的变换信息,就以越高的频度被执行验证,因此能够使针对篡改的风险又低又旧的对象变换信息的验证的频度变低。因此,由于能够按照篡改的风险来执行验证,从而能够在不使篡改的风险增大的状态下来减少验证的次数。因此,能够执行轻量级验证。

[0038] 另外,这些概括性的或具体的方式可以由系统、装置、集成电路、计算机程序或计算机可读的CD-ROM等记录介质来实现,也可以由系统、装置、集成电路、计算机程序以及记录介质的任意组合来实现。

[0039] (实施方式)

[0040] <概要>

[0041] 区块链系统作为虚拟货币Bitcoin的核心技术而具有知名度,其具备向Peer to Peer网络参加的多个节点。各节点拥有能够记录数据的账本,通过在多个节点间相互地对账本进行验证以及同步,从而账本的协调性在整个区块链系统上得到保证。

[0042] 这些多个节点通过账本,从而能够在区块链系统上进行日志数据的阅览、程序的登记以及执行。尤其是,该程序被称作智能合约。在智能合约中定义了执行条件或区块链上的处理内容,并且智能合约被登记到区块链。据此,能够将来自节点的要求即交易数据被存放到区块链作为触发,从而在账本上的智能合约的程序在区块链系统中被自动执行。

[0043] 此时的交易数据以及智能合约的数据被存放在被称作区块的单位中。在区块中通过利用密码学的散列函数来进行被变换的散列化,从而生成散列值。散列值是针对适用了密码学的散列函数的元数据的唯一的值,并且是从该散列值不能复原元数据的值。区块的散列值被存放到下一个被生成的区块。通过该处理被依次地反复,从而时间序列的链结构的区块链在网络全体的多个账本上被更新。

[0044] 区块链由于具有上述的时间序列的链结构,因此要想篡改账本上的一个数据,则不仅是需要改写该区块本身,还需要将不断增加的后续的区块在网络的一半以上的账本中进行改写。因此,可以说区块链的抗数据篡改性是高的。由于区块链具有高的抗篡改性,因此在金融、制造业等广泛的业界中被活用。进一步,随着近些年的数字市场的扩大,针对使必要的数据恰当地从拥有者向灵活运用的企业流通的“数据流通系统”,区块链也示出了有效性。

[0045] [数据流通系统]

[0046] 图1示出了实施方式所涉及的数据流通系统的构成的一个例子。

[0047] 本公开所涉及的数据流通系统1如图1所示,例如具备用户操作的信息终端10、以及多个服务器20a～服务器20c。这些由网络N来连接。网络N例如是互联网、便携式电话的承载网络等,可以由任意的通信线路或网络来构成。

[0048] 另外,以后将服务器20a～服务器20c也分别称作服务器20,还有将服务器20a～服务器20c称作服务器A～服务器C的情况。

[0049] 数据流通系统1例如向从信息终端10的浏览器进行接入的用户提供如下的5个功能,这5个功能是指:系统登录、系统退出、数据的加载、数据的下载、以及用户的权限设定。数据流通系统1提供与信息终端10的请求相应的功能。并且,数据流通系统1生成向信息终端10提供的功能的履历即操作日志,并将生成的操作日志记录到数据库21。操作日志由于与用户ID建立了对应,因此包括用户ID。数据流通系统1例如对操作日志中包括的用户ID进

行散列化,将包括散列化后的变换信息的日志交易数据记录到区块链22。

[0050] 并且,数据流通系统1在原始数据的加载或下载的功能被执行了的情况下,将原始数据存放到数据库21,对原始数据进行散列化,并将包括散列化后得到的散列值(变换信息)的日志交易数据存放到区块链22。在原始数据的加载或下载的功能被执行了的情况下,数据流通系统1对加载或下载的操作日志中包括的用户ID进行散列化,将包括散列化后的变换信息的日志交易数据记录到区块链22。

[0051] 另外,区块链平台例如可以采用Ethereum,关于共识算法,例如在以多个企业等具有利害关系的节点维持的网络中,可以预想到采用节点权限对等且容易维持抗篡改性的区块生成规则,因此采用Proof of Work(工作量证明)。区块生成与交易数据的发行频度无关,而以大约15秒的单位来执行。

[0052] [信息终端10]

[0053] 信息终端10接受由用户进行的操作,将与操作相应的请求发送到服务器20a～20c。信息终端10将用于使服务器20a～20c执行系统登录、系统退出、数据的加载、数据的下载、以及用户的权限设定这5个功能的请求,发送到服务器20a～20c。信息终端10在请求数据的加载的情况下,将成为加载的对象的数据发送到服务器20a～20c。信息终端10是设备的一个例子。请求是信息终端10进行工作而在信息终端10生成的信息,是日志信息的一个例子。请求也可以说是通过用户操作信息终端10而由信息终端10生成的信息(操作履历)。请求中包括用户ID。信息终端10将信息终端10进行工作而由信息终端10生成的多个日志信息,依次地发送给服务器20。

[0054] 图2示出了实施方式所涉及的信息终端的构成的一个例子。

[0055] 信息终端10具备通信部101、输入接受部102、显示部103、控制部104、以及存储部105。

[0056] 通信部101经由网络N将信息发送到服务器20,并且从服务器20接收信息。发送到服务器20的信息例如是用于使服务器20执行服务器20的功能的请求、加载的数据等。从服务器20接收的信息例如是从服务器20下载的数据等。通信部101每当请求被生成时,就将生成的请求发送给服务器20。通信部101在有加载的数据的情况下,将其与生成的请求一起发送给服务器20。

[0057] 这样,通信部101经由网络N与服务器20a～20c之间进行通信。另外,该通信可以由TLS(Transport Layer Security:传输层安全性协议)来实现,TLS通信用的加密密钥也可以在通信部101保持。

[0058] 输入接受部102接受通过用户的操作的信息输入。输入接受部102将接受的信息输入或者显示到显示部103、或者发送到控制部104、或者发送到通信部101。

[0059] 在本实施方式中,输入接受部102通过用户的操作,来接受示出使服务器20执行的功能的选择的信息输入。输入接受部102将接受的选择和用户的电子签名发送到控制部104。并且,输入接受部102通过用户的操作,来接受已确认到被显示在显示部103的通知。输入接受部102在将数据加载到服务器20的情况下,也可以接受加载的数据的选择。输入接受部102在从服务器20下载数据的情况下,也可以接受下载的数据的选择。

[0060] 显示部103对用于由输入接受部102接受输入的UI进行显示。并且,显示部103将输入接受部102接受的信息输入显示在UI。显示部103也可以显示从服务器20通知来的信息。

[0061] 控制部104根据由输入接受部102接受的信息输入,来生成请求,并将生成的请求经由通信部101发送给服务器20。

[0062] 存储部105对有可能成为加载的对象的数据进行存储。存储部105对下载的数据进行存储。

[0063] 信息终端10通过处理器利用存储器执行规定的程序来实现。

[0064] [服务器20]

[0065] 图3示出了实施方式所涉及的服务器的构成的一个例子。

[0066] 如图3所示,服务器20具备:通信部201、控制部202、记录部203、交易数据验证部204、数据库205、分布式账本206、以及智能合约执行部207。

[0067] 通信部201经由网络N或者将信息发送到信息终端10、或者从信息终端10接收信息。发送到信息终端10的信息例如是接受的针对服务器20的下载请求的数据等。从信息终端10接收的信息例如是使服务器20执行服务器20的功能的请求、向服务器20加载的数据等。

[0068] 并且,通信部201经由网络N与其他的服务器20之间进行通信。通信部201与其他的服务器20之间进行交易数据的收发。

[0069] 这样,通信部201经由网络N与信息终端10之间进行通信。另外,该通信可以通过TLS(Transport Layer Security)来实现,TLS通信用的加密密钥也可以由通信部201保持。

[0070] 另外,如以上所述,由于是信息终端10将通过信息终端10进行工作而由信息终端10生成的多个日志信息,依次地发送给服务器20,通信部201从信息终端10依次地获得该多个日志信息。获得的多个日志信息被依次地存放到数据库205。

[0071] 控制部202以规定的变换,将获得的多个日志信息分别变换为多个变换信息。规定的变换是将第1值唯一地变换为与第1值成为配对的第2值的具有再现性的方法,并且是不能从第2值变换为第1值的不可逆的变换。规定的变换例如是散列化。

[0072] 控制部202通过对多个日志信息的每一个进行规定的变换,从而生成多个变换信息。即控制部202对多个日志信息分别进行规定的变换,来一个一个地生成变换信息。控制部202生成包括被生成的变换信息的交易数据,并对生成的交易数据执行共识算法。据此,控制部202将多个变换信息依次地存放到区块链。

[0073] 并且,控制部202根据存放在数据库205的多个日志信息中的验证对象的对象日志信息、存放在区块链的多个变换信息中的对象变换信息,以规定的频度来执行对象日志信息以及对象变换信息的至少其中一方是否被篡改的验证。对象变换信息是多个变换信息中的与对象日志信息对应的变换信息。即对象变换信息是在服务器20获得了对象日志信息时,由控制部202对该对象日志信息进行规定的变换而生成的信息。

[0074] 控制部202在进行验证中,通过对对象日志信息以规定的变换进行变换,从而生成与已经存放到区块链的对象变换信息不同的例如验证用的变换信息。于是,控制部202对验证用的变换信息与区块链中存放的对象变换信息进行比较。控制部202在比较的结果为一致的情况下,判断为对象日志信息以及对象变换信息没被篡改,在比较的结果为不一致的情况下,判断为对象日志信息以及对象变换信息的至少其中一方被篡改。

[0075] 控制部202按照对象日志信息,对执行验证的规定的频度进行动态地变更。在日志信息的篡改中可以考虑到越是与不正当直接关联的日志信息的篡改则影响就更大。在上述

的服务器20的5个功能的情况下,与登录以及退出相比,可以说针对与个人信息泄漏等重大意外事件直接关联的用户的权限设定、数据的加载以及下载的日志信息的篡改的风险影响程度高。另外,由于该风险影响程度是基于操作类别的,因此是在日志生成后不发生变化的静态的参数。

[0076] 这样,按照对象日志信息的属性,篡改的风险影响程度会发生变化。因此,控制部202针对执行验证的规定的频度,在按日志信息的属性预先决定的重要度越高时,就决定越高的频度。多个日志信息的每一个,按日志信息的属性,被分类为多个级别的重要度。日志信息可以包括示出属性的标志。属性例如是示出系统登录、系统退出、数据的加载、数据的下载、以及用户的权限设定这5个功能的信息。

[0077] 例如,加载以及下载的日志信息被分类为重要度High,权限设定被分类为重要度Mid,登录以及退出被分类为重要度Low。重要度High是比重要度Mid高的重要度,重要度Mid是比重要度Low高的重要度。另外,以上虽然将重要度的分类定为3个级别,不过并非受此所限,也可以定为2个级别,或者可以是4个级别以上。

[0078] 并且,包括日志信息的交易数据针对作为数据库205的篡改检测中所使用的验证对象的数据而对应的日志信息,以组的方式被记录到区块链。因此,攻击者在对数据进行篡改时,需要对数据库205的日志信息、包括与该日志信息成为组的变换信息的区块、以及该区块之后的后续区块一并进行篡改。由于区块链的抗篡改性是源于需要对不断增加的后续区块进行改写,因此,在示出存放了变换信息的区块的位置的区块编号中,相对而言,区块编号越新时,则风险发生频度就越高。另外,该相对而言的区块编号所示的新旧是,以该区块编号相对于最新区块编号的比率来动态表现的参数,例如随着区块链的更新,而以15秒来更新一次。

[0079] 这样,按照存放了与对象日志信息相对应的对象变换信息的区块的新旧,篡改的风险发生频度则会发生变化。因此,控制部202以如下的方式来决定执行验证的规定的频度,即在包括与对象日志信息对应的对象变换信息的第1区块在区块链中的位置,离该区块链中最后连结的第2区块越近的情况下,就决定越高的频度。

[0080] 例如,控制部202进行如下的决定:对被存放到区块链的多个变换信息中的多个第1变换信息,以第1频度来进行验证,对多个第2变换信息,以第2频度来进行验证,对多个第3变换信息,以第3频度来进行验证。第1频度是比第2频度高的频度,第2频度是比第3频度高的频度。多个第1变换信息例如是多个变换信息之中在最新的一天存放到区块链的变换信息。多个第2变换信息例如是在最新的一天之前被存放的剩余的多个变换信息(即除了多个第1变换信息以外其余的多个变换信息)之中在第1期间存放的变换信息。多个第3变换信息例如是在第1期间以前的第2期间中存放的剩余的多个变换信息(即除了多个第1变换信息以及多个第2变换信息以外剩余的多个变换信息)。

[0081] 图4示出了区块链中的区块的位置。另外,在图4中朝下的三角形表示与日志信息对应的变换信息被生成的时刻。

[0082] 例如在Day2时,在Day2被存放的区块中包括的多个变换信息全都被设定为High(多个第1变换信息)。于是,Day1以前存放的区块之中新的一半的变换信息被设定为Mid(多个第2变换信息),旧的一半的变换信息被设定为Low(多个第3变换信息)。

[0083] 于是,在DayN时,在DayN被存放的区块中包括的多个变换信息全都被设定为High

(多个第1变换信息)。于是,在DayN以前存放的区块中的新的一半的变换信息被设定为Mid(多个第2变换信息),旧的一半的变换信息被设定为Low(多个第3变换信息)。

[0084] 另外,以上虽然是多个变换信息在区块链中的相对位置的分类被定为3个级别,不过并非受此所限,也可以定为2个级别,还可以定为4个级别以上。

[0085] 图5示出了决定规定的频度的表格的一个例子。

[0086] 如图5所示,规定的频度由表格来决定。表格以与多个组分别对应的多个频度来表现,所述多个组是以区块链的相对位置而分类的多个范围与重要度的级别的配对。具体而言,在表格中如图5所示那样示出了等级,在此的等级示出了与给风险影响程度造成影响的重要度和给风险发生频度造成影响的区块位置的组合对应的频度。等级Lv11、Lv12、Lv13、Lv21、Lv22、Lv23、Lv31、Lv32、Lv33可以是在表格的相邻的方格中彼此相等的情况,也可以按照满足重要度越高则具有高频度的倾向、且区块位置越新则具有高频度的倾向的方式,来决定各等级所表示的频度。例如可以是,Lv11、Lv12、Lv13被决定为高频度,Lv22、Lv23被决定为中频度,Lv21、Lv31、Lv32、Lv33被决定为低频度。另外,高频度是比中频度高的频度,中频度是比低频度高的频度。另外,频度并非受定为上述的3个级别所限,也可以定为2个级别,还可以定为4个级别以上。

[0087] 另外,日志信息也可以包括用于对表格中分类的组进行确定的标志。

[0088] 在此,返回到图3的说明。

[0089] 交易数据验证部204在通信部201接收到交易数据时,对该交易数据的正当性进行验证。例如,交易数据验证部204对通信部201所接收的交易数据中是否被赋予了以正确的方法生成的电子签名进行验证。另外,该验证也可以被跳过。

[0090] 并且,交易数据验证部204与多个其他的服务器20一起执行用于对交易数据的正当性达成协议的共识算法。

[0091] 在此的共识算法中可以采用PBFT(Practical Byzantine Fault Tolerance:实用拜占庭容错协议),也可以采用其他的周知的共识算法。作为周知的共识算法例如有PoW(Proof of Work)或PoS(Proof of Stake:持有量证明)等。在共识算法中采用PBFT的情况下,交易数据验证部204从多个服务器20的每一个接受示出交易数据的验证是否已成功的报告,并判断该报告的数量是否超过规定的数量。于是,交易数据验证部204在该报告的数量超过了规定的数量时,可以判断是否通过共识算法进行了交易数据的正当性的验证。

[0092] 交易数据验证部204在确认到交易数据的正当性的情况下,使该交易数据记录到记录部203。

[0093] 在本实施方式中,交易数据验证部204对通信部201所接收的交易数据的正当性进行验证。

[0094] 另外,记录部203将由交易数据验证部204进行了正当性的验证的交易数据包括在区块内来存放到分布式账本206,据此来记录交易数据。

[0095] 另外,记录部203也可以构成在分布式账本206的内部。

[0096] 在数据库205中存放多个日志信息。数据库205由存储装置来实现。

[0097] 在分布式账本206中存放交易数据。由于分布式账本206是依次获得交易数据并存放的,因此存放有1个以上的交易数据。分布式账本206由存储装置来实现。

[0098] 智能合约执行部207通过执行分布式账本206的被存放在区块链的交易数据中包

括的合约代码等,来使智能合约工作。智能合约执行部207可以通过使更新智能合约工作,来进行更新处理,该更新处理是将决定了规定的频度的表格更新为由更新交易数据指定的等级的处理。智能合约执行部207在分布式账本206内的区块链中被添加了包括更新交易数据的区块的情况下,也可以进行更新处理。

[0099] 这样,智能合约执行部207通过使智能合约工作,从而能够由分布式账本对更新处理进行管理。另外在此视为,更新智能合约例如根据来自用户的操作而由信息终端10的应用来生成,将包括这些智能合约的区块预先存放到区块链。即在区块链中存放有,在包括用于对表格进行更新的更新交易数据的区块被存放到区块链时,用来执行更新处理的更新智能合约的合约代码,所述更新处理是对表格中设定的多个频度进行更新的处理。

[0100] [工作]

[0101] 接着,对具有以上这种构成的数据流通系统1的工作进行说明。

[0102] 图6是示出实施方式所涉及的数据流通系统的工作的一个例子的流程图。

[0103] 服务器20从信息终端10依次地获得多个日志信息(S101)。

[0104] 接着,服务器20将多个日志信息存放到数据库205(S102)。

[0105] 接着,服务器20将获得的多个日志信息的每一个,以规定的变换来变换为多个变换信息(S103)。

[0106] 接着,服务器20生成包括被生成的变换信息的交易数据,并通过针对生成的交易数据与其他的服务器20一起执行共识算法,来将多个变换信息依次地存放到区块链(S104)。

[0107] 接着,服务器20根据被存放在数据库205的多个日志信息中的验证对象的对象日志信息、以及被存放在区块链的多个变换信息中的对象变换信息,以规定的频度来执行对象日志信息以及对象变换信息的至少其中一方是否被篡改的验证(S105)。

[0108] 图7是示出通过实施方式所涉及的数据流通系统进行的验证处理的一个例子的流程图。

[0109] 服务器20根据规定的频度,来决定验证对象的对象日志信息(S111)。例如可以是,服务器20在到了规定的验证定时的情况下,从被分类为表格中所决定的组的多个日志信息中,随机地提取与该组中设定的规定的频度相应的数量(比例)的日志信息,将提取的日志信息作为对象日志信息来决定。在此,规定的频度越大,就将提取的日志信息的数量(比例)决定得越大。换而言之,越增大随机地提取的日志信息的数量,就越能够增高被分类为组的日志信息的验证频度。并且,例如也可以是,服务器20以基于表格的规定的频度,对各日志信息决定验证计划,将到了验证计划中决定的时期的日志信息作为对象日志信息来决定。

[0110] 接着,服务器20以规定的变换来对对象日志信息进行变换,与已经被存放到区块链的对象变换信息无关地来生成验证用的变换信息(S112)。

[0111] 接着,服务器20从区块链中获得与对象日志信息对应的对象变换信息(S113)。

[0112] 接着,服务器20对验证用的变换信息与被存放在区块链的对象变换信息进行比较(S114)。

[0113] 于是,服务器20在比较的结果为一致的情况下(S115的“是”),判断为对象日志信息以及对象变换信息没被篡改(S116)。

[0114] 服务器20在比较的结果为不一致的情况下(S115的“否”),则判断为对象日志信息

以及对象变换信息的至少其中一方被篡改(S117)。

[0115] [实施例]

[0116] 图8以及图9是用于说明数据流通系统的工作的具体例子的图。

[0117] 在数据流通系统1中,例如针对医疗保健的个人数据等重要信息,需要在保护个人隐私的状态下,在众多的用户间以高的可靠性来对待。在这种情况下,包括重要信息的原始数据以及数据流通系统1中的操作履历即操作日志的数据23被记录到仅持有权限的用户才能使用的关闭的数据库21的同时,也将经过个人隐私保护加工(变换)后的加工数据24(变换信息)记录到其他的用户也能够阅览的开放的区块链22。也就是说,数据23成为没有经过个人隐私保护加工的数据23与经过个人隐私保护加工后的加工数据24的组,被分别记录到关闭的数据库21和开放的区块链22。另外,数据库21与数据库205相同。

[0118] 例如图9的(1)所示,在通过用户操作加载了原始数据时,则原始数据被存放到数据库21。于是,如图9的(2)所示,加载了原始数据的日志信息被生成,日志信息被存放到数据库21。并且,如图9的(3)所示,服务器20将原始数据以及日志信息进行散列化。于是,如图9的(4)所示,服务器20将包括通过散列化而生成的加工数据24的交易数据记录到区块链。

[0119] 于是,被记录在数据库21以及区块链22这双方的数据23以及加工数据24以形式统一的状态而被比较(以后视为“验证”),接受双方的某一方是否被篡改的篡改检测。具体而言,如图9的(5)所示,服务器20在验证中,通过对数据库21中存放的数据23进行与将数据存放到区块链时进行的个人隐私保护加工相同的处理,来生成验证用的加工数据25(变换信息),据此,将数据23的形式变换为与区块链22中存放的加工数据26相同的形式。于是如图9的(6)所示,服务器20通过对验证用的加工数据25与加工数据26进行比较,来进行验证。据此,不是将重要信息本身记录到区块链,而是能够间接地提高系统自身的可靠性。

[0120] 另外,个人隐私保护加工例如是散列化。也就是说,在个人隐私保护加工中可以采用如下的方法,即通过对元数据利用密码学的散列函数来进行变换,对适用了密码学的散列函数的元数据生成唯一的值,且该唯一的值是不能从该散列值复原元数据的散列值。

[0121] 因内部不正当而造成的数据的篡改与外部攻击不同,因此想要预测何时在哪儿发生是困难的。并且,由于内部不正当是因持有权限的用户造成的不正当,因此风险大。为了将这种数据的篡改造成的危害抑制到最小,从而需要在发现意外事件前,系统能够迅速地检测因内部不正当造成的数据的篡改。并且,在进行上述的验证的情况下,由于是间接地对数据库上的数据的篡改进行检测,因此不是对最近的,而是需要对保存期间中所有的数据进行高频度地验证。

[0122] 在从系统监察的观点来看,数据被赋予长期保存的义务,因此可以预想到存放有成为验证对象的数据的数据库以及区块链都需要长期地进行数据更新且保存。据此,若针对被记录的所有的数据高频度地进行验证,则计算量会随着时间的经过而增大,在长期的运用中将成为课题。

[0123] 于是,在数据流通系统1中,在存放的数据增大的条件下,按照数据的类别和区块链的时间序列结构来高效地选择验证对象,通过对验证频度进行动态地变更,从而实现了能够对篡改进行轻量级检测的验证方法。

[0124] [效果等]

[0125] 通过本实施方式所涉及的验证方法,服务器20通过信息终端10进行工作,从而从

信息终端10依次地获得在该信息终端生成的多个日志信息。服务器20将多个日志信息依次地存放到数据库205,且将多个日志信息以规定的变换来分别进行变换,将变换后的多个变换信息依次地存放到区块链。服务器20根据多个日志信息中的验证对象的对象日志信息、以及多个变换信息中的与对象日志信息对应的对象变换信息,以规定的频度来执行对象日志信息以及对象变换信息的至少其中一方是否被篡改的验证。规定的频度以如下的方式来决定,即在对象变换信息被存放到区块链的时刻越接近进行验证的当前时刻,就决定越高的频度。

[0126] 据此,对象变换信息在区块链中被存放的时刻越接近进行验证的当前时刻,就以越高的频度来执行针对该对象变换信息的验证,从而能够降低篡改的风险低且旧的对象变换信息进行验证的频度。这样,由于能够按照篡改的风险来执行验证,因此不会增大篡改的风险,就能够减少验证的次数。因此,能够执行轻量级验证。

[0127] 并且,在本实施方式所涉及的验证方法中,规定的频度以如下的方式来决定,即包括对象变换信息的第1区块在区块链中的位置离区块链中最后连结的第2区块越近,就决定越高的频度。

[0128] 因此,越是对象变换信息在区块链中被存放的时刻离进行验证时的当前时刻近的区块中包括的变换信息,就越以高的频度来进行验证,因此能够降低对篡改的风险低且旧的对象变换信息进行验证的频度。

[0129] 并且,在本实施方式所涉及的验证方法中,多个日志信息的每一个被分类为按日志信息的属性而预先决定的多个级别的重要度。规定的频度以如下的方式来决定,即包括对象变换信息的区块在区块链中的位置离区块链中最后连结的第2区块越近,就决定越高的频度,并且重要度越高,就决定越高的频度。

[0130] 因此,越是对象变换信息在区块链中被存放的时刻离进行验证时的当前时刻近的区块中包括的变换信息,就越以高的频度来执行验证,因此能够降低对篡改的风险低且旧的对象变换信息进行验证的频度。并且,由于能够进一步按日志信息的属性,来设定给规定的频度带来影响的重要度,因篡改而风险影响程度越高的日志信息,就以越高的频度来执行验证。

[0131] 并且,在本实施方式所涉及的验证方法中,规定的频度由表格来决定。表格以与多个组分别对应的多个频度来表现,所述多个组是以区块链的相对位置来分类的多个范围与重要度的级别的配对。因此,通过参照表格,从而能够决定规定的频度。

[0132] 并且,在本实施方式所涉及的验证方法中,区块链中存放有如下的智能合约,该智能合约是在包括用于更新表格的交易数据的区块被存放到区块链时,用来执行对表格中设定的多个频度进行更新的更新处理的智能合约。

[0133] 据此,能够以交易数据被存放区块链为契机,利用智能合约来自动更新表格。并且,由于能够通过更新表格来对规定的频度进行更新,因此能够减轻对规定的频度进行更新的处理中所需要的处理负荷。

[0134] 并且,在本实施方式所涉及的验证方法中,服务器20在进行验证时,通过以规定的变换来对对象日志信息进行变换,从而生成验证用的变换信息。服务器20对验证用的变换信息与区块链中存放的对象变换信息进行比较。服务器20在比较的结果为一致的情况下,判断为对象日志信息以及对象变换信息没被篡改,在不一致的情况下,判断为对象日志信

息以及对象变换信息的至少其中一方被篡改。

[0135] 并且,在本实施方式所涉及的验证方法中,规定的变换是将第1值变换为与第1值配对的第2值的具有再现性的方法,并且所述规定的变换是不能从第2值变换为第1值的不可逆的变换。

[0136] 因此,能够提高用于对数据库中存放的数据进行验证的、被存放在开放的区块链的数据的匿名性。

[0137] [其他的实施方式等]

[0138] 以上虽然基于实施方式对本公开进行了说明,但是本公开并非受上述的实施方式所限。以下的情况也包括在本公开中。

[0139] (1)在上述实施方式中,虽然是信息终端10向服务器20发送多个日志信息,但是,发送多个日志信息的设备并非受信息终端10所限,也可以是具有通信功能的家电设备。

[0140] (2)在上述实施方式中,虽然是根据表格并按照区块的位置以及日志信息的属性,来决定规定的频度的,但是并非受此所限,也可以按照区块的位置以及日志信息的属性的一方来决定规定的频度。即在按照区块的位置来决定规定的频度的情况下,在规定的频度的决定中也可以不利用日志信息的属性。并且,在按照日志信息的属性来决定规定的频度的情况下,在规定的频度的决定中也可以不利用区块的位置。并且,只要包括对象变换信息的第1区块在区块链中的位置离区块链中最后连结的第2区块越近,就决定越高的频度,规定的频度的决定中也可以不利用表格。并且也可以是,在规定的频度的决定中,只要是重要度越高就决定越高的频度,也可以不利用表格。

[0141] (3)在上述实施方式中,虽然是通过具有存放了区块链的分布式账本的服务器20来进行日志信息的验证的,但是并非受此所限,也可以由与服务器20不同的外部的装置来进行日志信息的验证。

[0142] (4)在上述实施方式中,虽然示出了数据库205和分布式账本206被设置在相同的服务器20的例子,但是并非受此所限,数据库205和分布式账本206也可以设置在不同的装置。

[0143] (5)在上述实施方式中,验证的频度可以通过原始数据的种类来决定。例如,也可以是与原始数据示出人的属性的静态的个人信息相比,以示出人的生物信息的动态的个人信息的验证频度高的方式来决定。

[0144] (6)在上述实施方式中,执行验证的期间也可以被设定为一天之中的夜晚等特定的期间。在这种情况下,特定的期间的长度可以按每天来变更,在这种情况下,执行的验证的次数可以按照特定的期间的长度来动态地变更。即验证的次数可以按照每单位时间执行验证的次数不变的方式来决定。

[0145] (7)在上述实施方式中,关于与进行验证时的当前时刻相比在规定时间以上旧的期间生成的多个日志信息,可以作为存档而被压缩成1个数据。在这种情况下,可以将被压缩的数据与日志信息同样对待。也就是说,可以将被压缩的数据存放到数据库205,将被压缩的数据的散列值存放到区块链。

[0146] (8)上述的实施方式中的各装置具体而言是由微处理器、ROM、RAM、硬盘单元、显示器单元、键盘、鼠标等构成的计算机系统。在所述RAM或硬盘单元中记录有计算机程序。通过所述微处理器按照所述计算机程序来工作,从而各装置实现其功能。在此,计算机程序为了

实现规定的功能,示出针对计算机的指令的指令代码由多个组合构成。

[0147] (9)上述的实施方式中的各装置中的构成要素的一部分或全部可以由一个系统LSI(Large Scale Integration:大规模集成电路)来构成。系统LSI是多个的构成部集成在一个芯片上而被制造的超多功能LSI,具体而言,是包括微处理器、ROM、RAM等来而被构成的计算机系统。在所述RAM中记录有计算机程序。通过所述微处理器按照所述计算机程序来工作,从而系统LSI实现其功能。

[0148] 并且,构成上述的各装置的构成要素的各个功能部可以分别被制成一个芯片,也可以是其中的一部分或全部被制成一个芯片。

[0149] 并且,在此虽然是系统LSI,不过根据集成的程度的不同,也有称为IC、LSI、超级LSI、极超级LSI的情况。并且,集成电路化的方法并非受LSI所限,也可以由专用电路或通用处理器来实现。也可以利用在LSI制造后可编程的FPGA(Field Programmable Gate Array:现场可编程门阵列)、LSI内部的电路单元的连接或设定可重构的可重装处理器。

[0150] 而且,伴随着半导体技术的进步或派生出其他的技术,而出现了替代LSI的集成电路化的技术的情况下,当然也可以利用这些技术来进行功能区块的集成化。也会有适用生物技术等的可能性。

[0151] (10)构成上述的各装置的构成要素的一部分或全部可以由能够装拆于各装置的IC卡或单体模块来构成。所述IC卡或所述模块是由微处理器、ROM、RAM等构成的计算机系统。所述IC卡或所述模块可以包括上述的超多功能LSI。通过微处理器按照计算机程序来进行工作,从而所述IC卡或所述模块实现各自的功能。该IC卡或该模块也可以具有防篡改性。

[0152] (11)本公开也可以是以上所示的方法。并且,可以作为由计算机来实现这些方法的计算机程序来实现,还可以作为由所述计算机程序构成的数字信号来实现。

[0153] 并且,本公开也可以作为记录了所述计算机程序或所述数字信号的计算机可读的记录介质来实现,所述记录介质例如是软盘、硬盘、CD-ROM、MO、DVD、DVD-ROM、DVD-RAM、BD(Blu-ray(注册商标)Disc)、半导体存储器等。并且,也可以作为被记录在这些记录介质的所述数字信号来实现。

[0154] 并且,本公开可以将所述计算机程序或所述数字信号经由电子通信线路、无线或有线通信线路、以互联网为代表的网络、数据播放等来传输。

[0155] 并且,本公开可以是具备微处理器和存储器的计算机系统,所述存储器中存储上述的计算机程序,所述微处理器按照所述计算机程序来工作。

[0156] 并且,可以通过将所述程序或所述数字信号记录到所述记录介质来传送,或者通过将所述程序或所述数字信号经由所述网络等来传送,据此,可以通过独立的其他的计算机系统来执行。

[0157] (12)也可以对上述实施方式以及上述变形例分别进行组合。

[0158] 本公开能够用于验证方法、服务器、以及程序,例如能够利用于能够执行轻量级验证的验证方法、服务器、以及程序等。

[0159] 符号说明

[0160] 1 数据流通系统

[0161] 10 信息终端

[0162] 20、20a、20b、20c 服务器

[0163] 21 数据库

[0164] 22 区块链

[0165] 23 数据

[0166] 24～26 加工数据

[0167] 101、201 通信部

[0168] 102 输入接受部

[0169] 103 显示部

[0170] 104、202 控制部

[0171] 105 存储部

[0172] 203 记录部

[0173] 204 交易数据验证部

[0174] 205 数据库

[0175] 206 分布式账本

[0176] 207 智能合约执行部

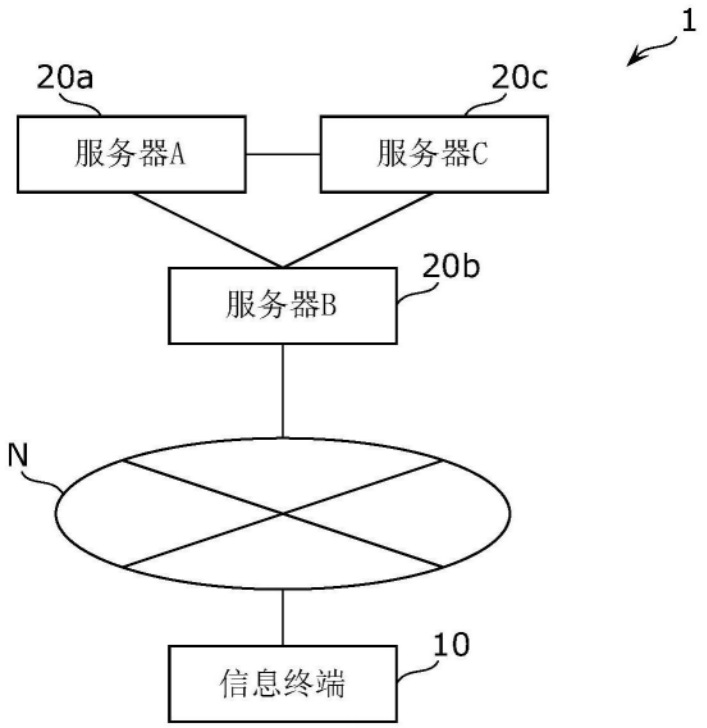

1
20a
20c
服务器A
服务器C
20b
服务器B
N
10
信息终端

图1

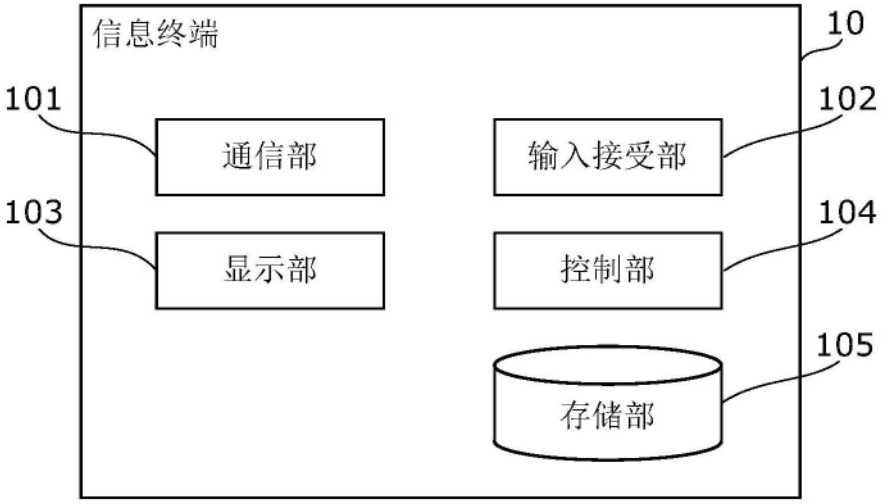

信息终端
10
101
通信部
102
输入接受部
103
显示部
104
控制部
105
存储部

图2

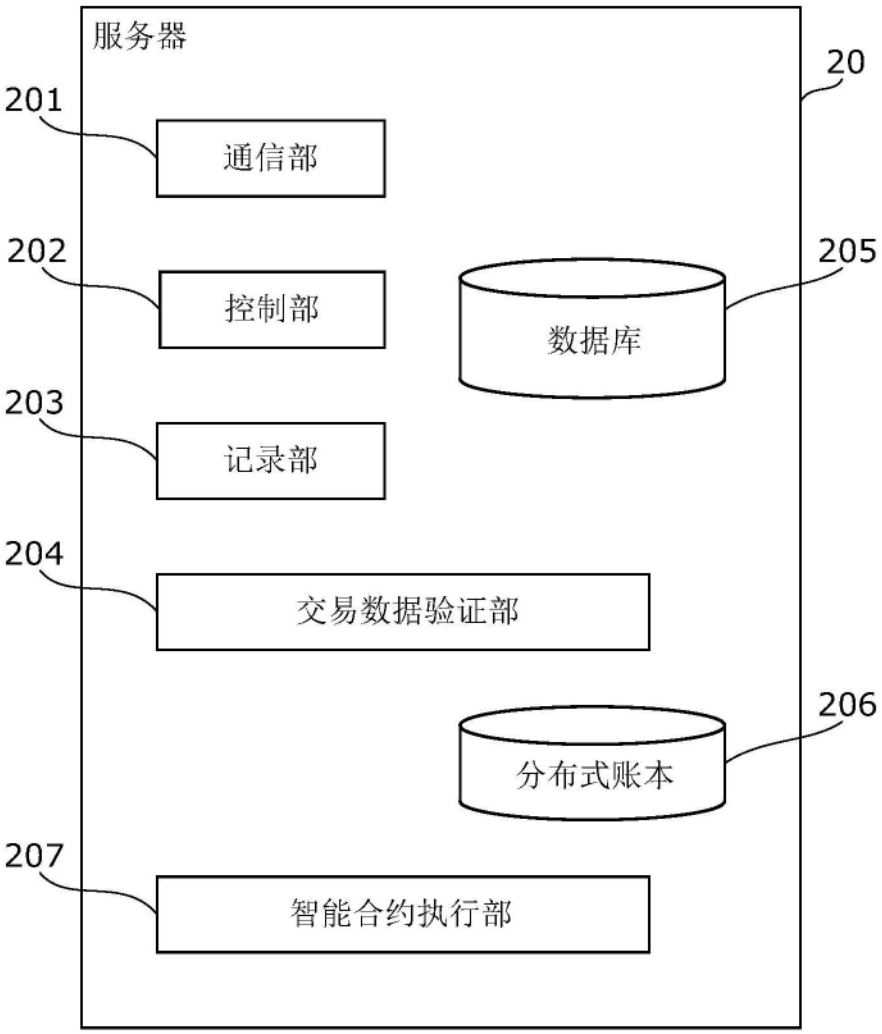

服务器
20
201
通信部
202
控制部
205
数据库
203
记录部
204
交易数据验证部
206
分布式账本
207
智能合约执行部

图3

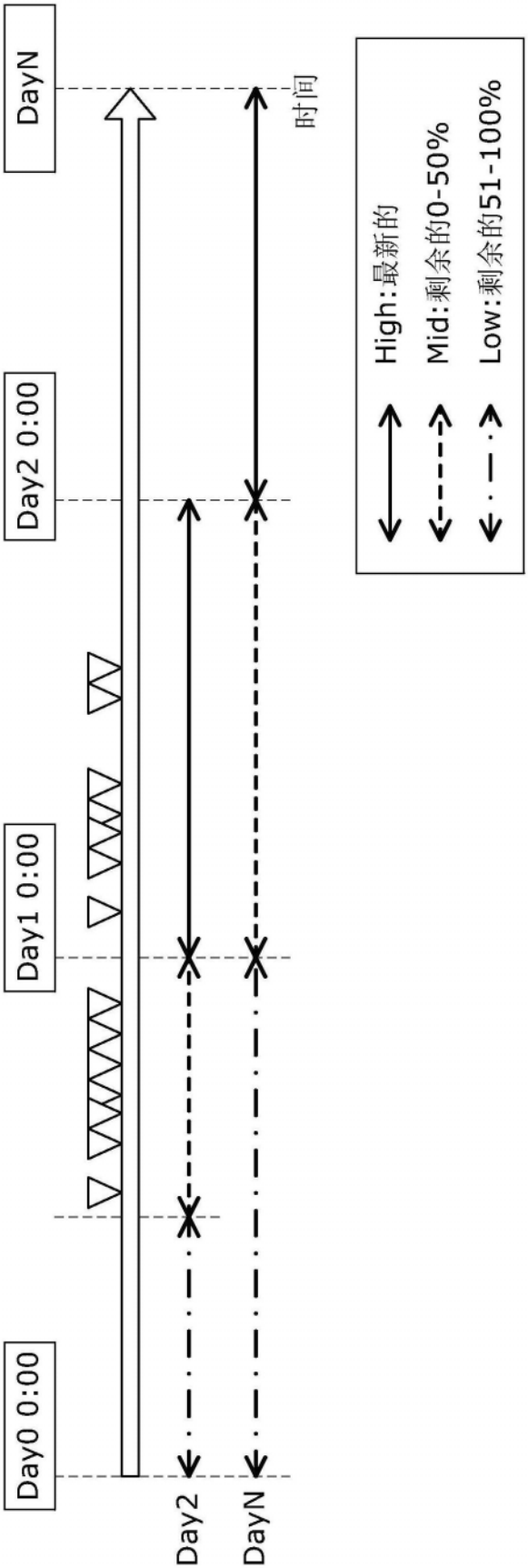

DayN
Day2 0:00
Day1 0:00
Day0 0:00
时间
High:最新的
Mid:剩余的0-50%
Low:剩余的51-100%
Day2
DayN

图4

重要度 / 区块位置	Low	Mid	High
High (a=1/N)	Lv11 (x/N)	Lv12 (y/N)	Lv13 (z/N)
Mid (b=(N-1)/2N)	Lv21 (x/(N-1)/2N)	Lv22 (y/(N-1)/2N)	Lv23 (z/(N-1)/2N)
Low (d=(N-1)/2N)	Lv31 (x/(N-1)/2N)	Lv32 (y/(N-1)/2N)	Lv33 (z/(N-1)/2N)

图5

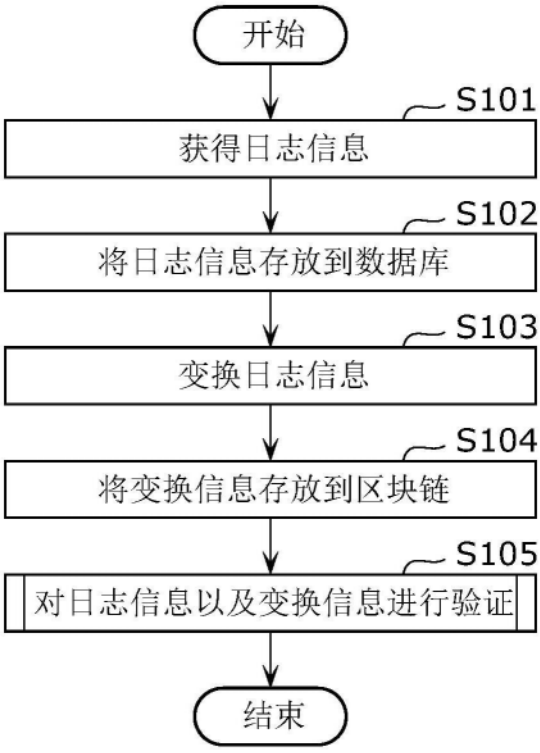


图6

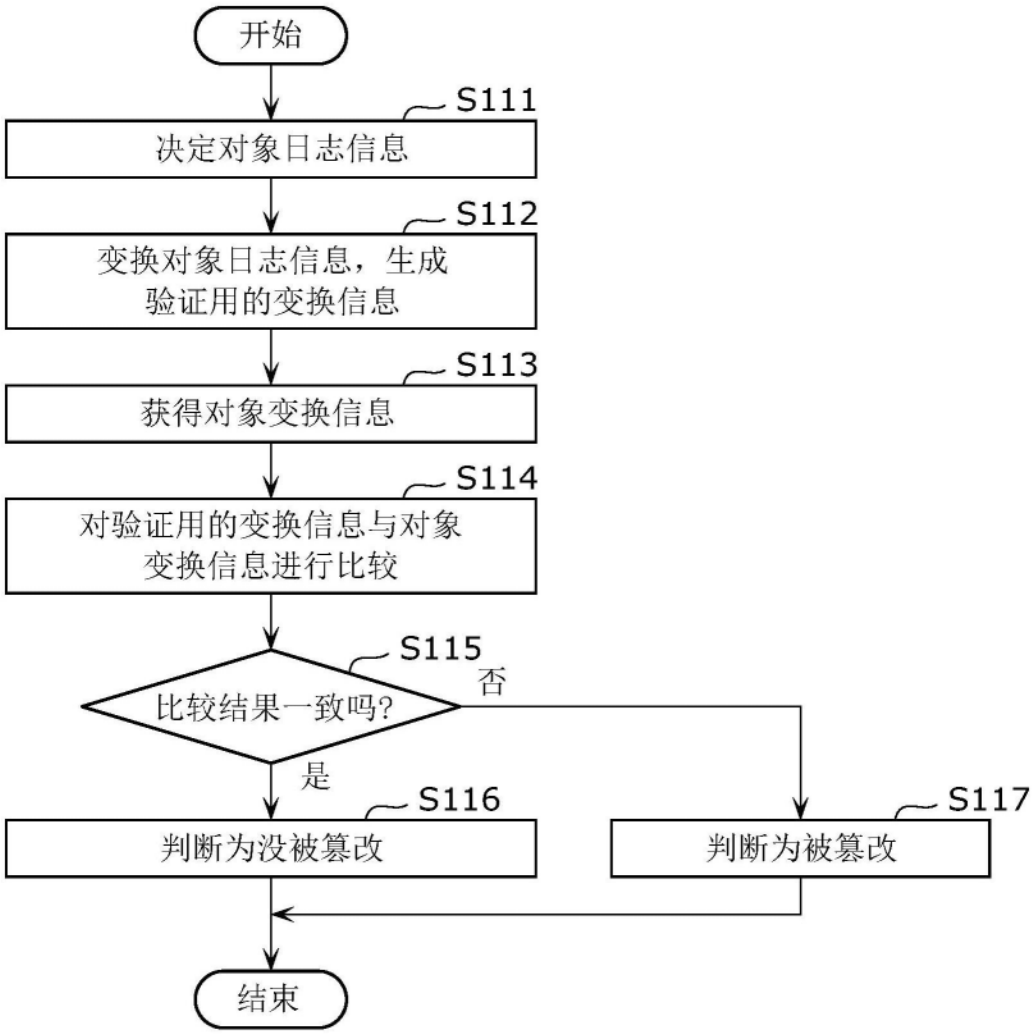

开始
S111
决定对象日志信息
S112
变换对象日志信息，生成
验证用的变换信息
S113
获得对象变换信息
S114
对验证用的变换信息与对象
变换信息进行比较
S115
比较结果一致吗?
否
是
S116
判断为没被篡改
S117
判断为被篡改
结束

图7

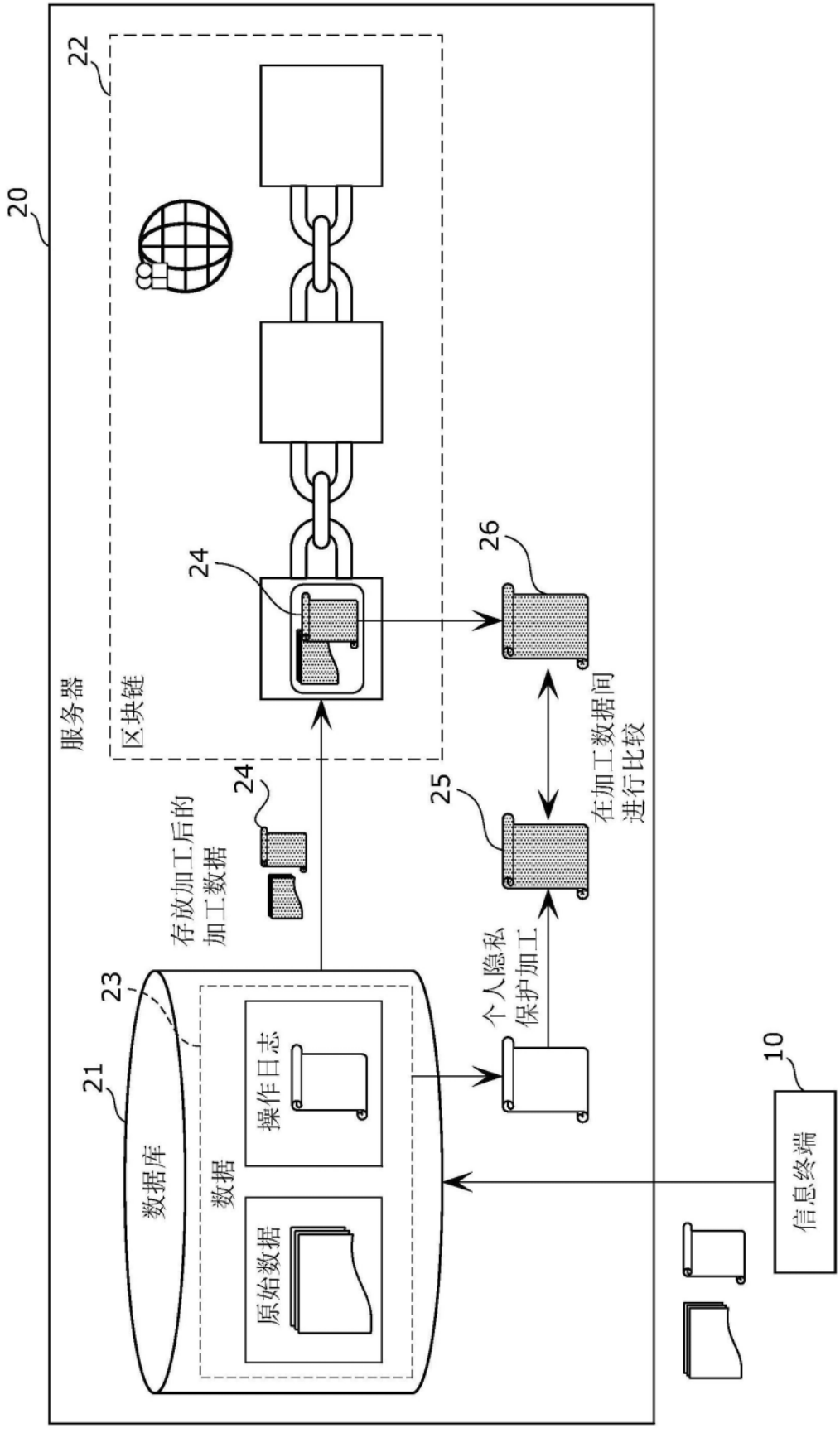

20
服务器
22
区块链
24
26
25
24
存放加工后的
加工数据
在加工数据间
进行比较
23
21
数据库
数据
操作日志
原始数据
个人隐私
保护加工
10
信息终端

图8

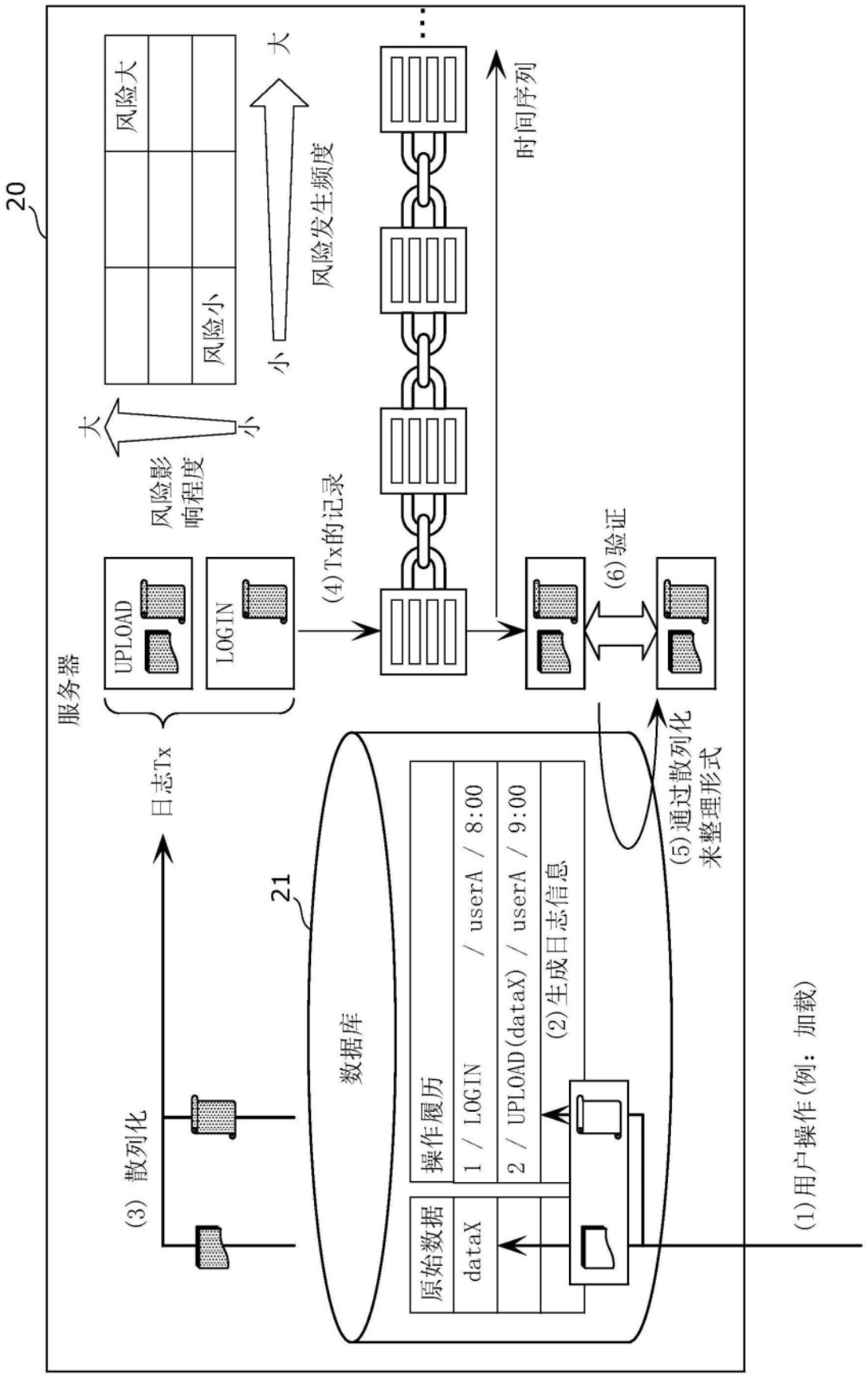

20
服务器
UPLOAD
LOGIN
日志Tx
(3) 散列化
21
数据库
原始数据
dataX
操作履历
1 / LOGIN / userA / 8:00
2 / UPLOAD(dataX) / userA / 9:00
(2)生成日志信息
(1)用户操作(例：加载)
(4)Tx的记录
(5)通过散列化
来整理形式
(6)验证
时间序列
风险发生频度
小
大
风险影
响程度
大
小
风险小
风险大

图9