(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 113785282 A
(43)申请公布日 2021.12.10

(21)申请号 202080030658.0

(22)申请日 2020.04.24

(30)优先权数据
62/838,436 2019.04.25 US

(85)PCT国际申请进入国家阶段日
2021.10.22

(86)PCT国际申请的申请数据
PCT/JP2020/017789 2020.04.24

(87)PCT国际申请的公布数据
WO2020/218550 JA 2020.10.29

(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 西田直央 海上勇二 道山淳儿

(74)专利代理机构 永新专利商标代理有限公司 72002
代理人 安香子

(51)Int.Cl.
G06F 16/182(2006.01)

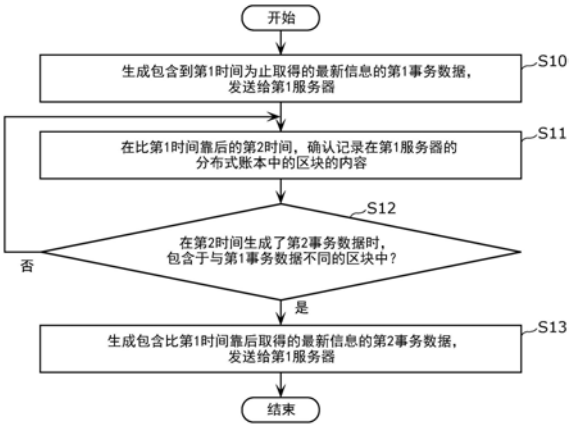
权利要求书2页 说明书13页 附图13页

(54)发明名称

控制方法、数据生成装置及程序

(57)摘要

控制方法生成包含到第1时间为止取得的最新信息的第1事务数据,发送给多个服务器中的第1服务器(S10);通过在比第1时间靠后的1个以上的第2时间确认记录在第1服务器的分布式账本中的区块的内容,来确认在第2时间生成了第1事务数据的后一个的第2事务数据时,第1事务数据被记录到分布式账本中时被包含于的第1区块与第2事务数据被记录到分布式账本中时被包含于的第2区块是否不同(S11);在第1区块与第2区块不同的情况下(S12中是),在该第2时间以后生成包含比第1时间靠后取得的最新信息的第2事务数据,发送给第1服务器(S13)。



CN 113785282 A

1.一种控制方法,是在具备设备和多个服务器的系统中由上述设备执行的控制方法,所述多个服务器分别与上述设备可通信地连接,并按每规定的定时,将在到该规定的定时为止所保持的事务数据中选择的事务数据包含于区块中并记录到分布式账本,其中,

在该控制方法中,

生成包含到第1时间为止取得的最新信息的第1事务数据,发送给上述多个服务器中的第1服务器,

通过在比上述第1时间靠后的1个以上的第2时间确认记录在上述第1服务器的上述分布式账本中的区块的内容,来确认在上述第2时间生成了上述第1事务数据的后一个的第2事务数据时,上述第1事务数据被记录到上述分布式账本中时被包含于的第1区块与上述第2事务数据被记录到上述分布式账本中时被包含于的第2区块是否不同,

在上述第1区块与上述第2区块不同的情况下,在该第2时间以后生成包含比上述第1时间靠后取得的最新信息的上述第2事务数据,发送给上述第1服务器。

2.如权利要求1所述的控制方法,其中,

在确认上述区块的内容时,确认作为上述区块的内容,在上述区块中是否包含有在上述第1事务数据的前一个生成的第3事务数据。

3.如权利要求2所述的控制方法,其中,

还取得上述第1服务器每单位时间接收的事务数据数即接收总数、以及上述第1服务器向上述分布式账本记录时每单位时间能够处理的事务数据数即可处理数,

在上述可处理数为根据上述接收总数设定的阈值以上的情况下,确认作为上述区块的内容,在上述区块中是否包含有上述第3事务数据。

4.如权利要求1所述的控制方法,其中,

在确认上述区块的内容时,确认作为上述区块的内容,在上述区块中是否包含有上述第1事务数据。

5.如权利要求3或4所述的控制方法,其中,

还取得上述第1服务器每单位时间接收的事务数据数即接收总数、以及上述第1服务器向上述分布式账本记录时每单位时间能够处理的事务数据数即可处理数,

在上述可处理数比根据上述接收总数设定的阈值小的情况下,确认作为上述区块的内容,在上述区块中是否包含有上述第1事务数据。

6.一种数据生成装置,与多个服务器可通信地连接,所述多个服务器分别按每规定的定时,将在到该规定的定时为止保持的事务数据中选择的事务数据包含于区块中并记录到分布式账本,其中,

上述数据生成装置具备:

处理器;以及

存储器,

上述处理器生成包含到第1时间为止取得的最新信息的第1事务数据,发送给上述多个服务器中的第1服务器;

上述处理器通过在比上述第1时间靠后的1个以上的第2时间确认记录在上述第1服务器的上述分布式账本中的区块的内容,来确认在上述第2时间生成了上述第1事务数据的后一个的第2事务数据时,上述第1事务数据被记录到上述分布式账本中时被包含于的第1区

块与上述第2事务数据被记录到上述分布式账本中时被包含于的第2区块是否不同；

上述处理器在确认到上述第1区块与上述第2区块不同的情况下，在该第2时间以后生成包含比上述第1时间靠后取得的最新信息的上述第2事务数据，发送给上述第1服务器。

7.一种程序，用来使计算机执行在具备设备和多个服务器的系统中由上述设备执行的控制方法，所述多个服务器分别与上述设备可通信地连接，并按每规定的定时，将在到该规定的定时为止保持的事务数据中选择的事务数据包含于区块中并记录到分布式账本，其中，

所述程序用来使计算机执行以下处理：

生成包含到第1时间为止取得的最新信息的第1事务数据，发送给上述多个服务器中的第1服务器，

通过在比上述第1时间靠后的1个以上的第2时间确认记录在上述第1服务器的上述分布式账本中的区块的内容，来确认在上述第2时间生成了上述第1事务数据的后一个的第2事务数据时，上述第1事务数据被记录到上述分布式账本中时被包含于的第1区块与上述第2事务数据被记录到上述分布式账本中时被包含于的第2区块是否不同；

在确认到上述第1区块与上述第2区块不同的情况下，在该第2时间以后生成包含比上述第1时间靠后取得的最新信息的上述第2事务数据，发送给上述第1服务器。

控制方法、数据生成装置及程序

技术领域

[0001] 本公开涉及控制方法、数据生成装置及程序。

背景技术

[0002] 作为从比特币产生的技术，有区块链技术(例如参照非专利文献1)。区块链是每隔一定时间生成被称作区块的数据单位并通过如链那样连结来保管数据的数据库。通过利用区块链，以谁都能够参加的对等(Peer to Peer:P2P)网络来共享交易履历(事务(transaction)数据)并相互监视，从而能够担保可靠性，防止数据的篡改。

[0003] 另外，在非专利文献1所记载的比特币的区块链中，区块的尺寸被限制为1MB，区块生成间隔被设为约10分钟。

[0004] 因此，也进行如下处理:变更区块链的规格，将区块生成间隔设为约2分钟，从而增加数据的处理量(例如参照非专利文献2)

[0005] 现有技术文献

[0006] 非专利文献

[0007] 非专利文献1:Satoshi Nakamoto,“Bitcoin:A Peer-to-Peer Electronic Cash System”,2009

[0008] 非专利文献2:BitcoinCandy,“Bitcoin Candy Whitepaper”,(https://cdy.one/whitepaper.pdf)

发明内容

[0009] 发明要解决的课题

[0010] 此外，在非专利文献1及非专利文献2所记载的区块链中，在1个区块中包含多个事务数据来生成。因此，根据区块生成间隔，有由相同的用户或相同的厂商在多个时间点发送的多个事务数据包含于1个区块的情况。

[0011] 但是，根据事务数据中包含的信息的种类，有即使在1个区块中包含由相同的用户或相同的厂商在多个时间点发送的多个事务数据也没有意义的情况。举例来讲，是以下情况:在仅将区块链中记录的最新的天气信息作为参考而决定价格的情况下，最新以外的天气信息也包含于1个区块。即为在区块中包含的多个事务数据之中仅利用包含最新信息的事务数据，而不利用包含过去的信息的事务数据的情况。在这样的情况下，在区块链的区块中会记录不利用的无用的事务数据。这不仅成为有限的网络带宽的浪费使用，也成为包括区块生成的电力等的资源的浪费使用。

[0012] 本公开是鉴于上述的情况而做出的，目的是提供一种能够抑制网络带宽及资源的浪费使用的控制方法等。

[0013] 用来解决课题的手段

[0014] 为了达成上述目的，本公开的控制方法，是在具备设备和多个服务器的系统中由上述设备执行的控制方法，所述多个服务器分别与上述设备可通信地连接，并按每规定的

定时，将在到该规定的定时为止保持的事务数据中选择的事务数据包含于区块中并记录到分布式账本，在该控制方法中，生成包含到第1时间为止取得的最新信息的第1事务数据，发送给上述多个服务器中的第1服务器，在比上述第1时间靠后的1个以上的第2时间，通过确认记录在上述第1服务器的上述分布式账本中的区块的内容，来确认在上述第2时间生成了上述第1事务数据的后一个的第2事务数据时，上述第1事务数据被记录到上述分布式账本中时被包含于的第1区块与上述第2事务数据被记录到上述分布式账本中时被包含于的第2区块是否不同，在上述第1区块与上述第2区块不同的情况下，在该第2时间以后生成包含比上述第1时间靠后取得的最新信息的上述第2事务数据，发送给上述第1服务器。

[0015] 另外，这些包含性或具体的技术方案也可以由系统、方法、集成电路、计算机程序或计算机可读取的CD－ROM等的记录介质实现，也可以由系统、方法、集成电路、计算机程序及记录介质的任意的组合来实现。

[0016] 发明效果

[0017] 根据本公开的控制方法等，能够抑制网络带宽及资源的浪费使用。

附图说明

[0018] 图1是表示区块链的概念的说明图。

[0019] 图2是表示图1所示的区块链的数据结构的说明图。

[0020] 图3是以图1所示的区块链的区块生成间隔进行的处理的说明图。

[0021] 图4是表示通过执行图3所示的共识算法进行的处理的流程图的一例。

[0022] 图5是示意地表示有关实施方式的控制系统的构成的图。

[0023] 图6是示意地表示有关实施方式的设备的构成的框图。

[0024] 图7是表示通过软件实现有关实施方式的设备的功能的计算机的硬件构成的一例的图。

[0025] 图8是表示有关实施方式的认证服务器装置的功能构成的框图。

[0026] 图9是表示有关实施方式的设备的动作的流程图。

[0027] 图10是有关实施例1的控制系统的处理的顺序图。

[0028] 图11是表示有关实施例2的设备的处理的流程图。

[0029] 图12是用来对有关实施方式的效果进行说明的流程图。

[0030] 图13是用来对有关实施方式的效果进行说明的流程图。

[0031] 图14是图13所示的流程图的其他观点下的说明图。

具体实施方式

[0032] (作为本公开的基础的认识)

[0033] 首先，对区块链进行说明。

[0034] 图1是表示区块链的概念的说明图。

[0035] 区块链是以“1个区块”为记录单位将区块以链(chain)状相连而成的，被记录到分布式账本。在图1中，表示了将在时间上比区块B0靠后生成的区块B1与区块B0连接、将在时间上比区块B1靠后生成的区块B2与区块B1连接……的例子。即，在图1中表示了区块B0～区块B3以链状相连的区块链的例子。

[0036] 图2是表示图1所示的区块链的数据结构的说明图。

[0037] 图1所示的区块链的区块具有多个事务数据和紧前的区块的哈希值。具体而言，在区块B2中包含其之前的区块B1的哈希值。并且，根据区块B2中包含的多个事务数据和区块B1的哈希值运算出的哈希值作为区块B2的哈希值被包含于区块B3。

[0038] 像这样，在区块链技术中，将之前的区块的内容作为哈希值来包含，并且将区块以链状连接，从而有效地防止所连接的事务数据的篡改。这是因为，假如过去的事务数据被变更，则区块的哈希值成为与变更前不同的值。要想将篡改后的区块伪装成正确的区块，必须重新制作其以后的全部区块，该作业在现实中是非常困难的，所以事实上可以说是不能篡改的。进而，记录区块链的分布式账本分别设置于在物理上不同的许多个据点，所以即使发生对某地点的账本的篡改，也能够根据其他账本检测出篡改。据此也可以说区块链事实上是不能篡改的。

[0039] 接着，使用附图对区块生成间隔中的处理即生成区块并连接到(写入)区块链为止的处理进行说明。另外，生成区块并写入区块链写入为止的处理，相当于生成区块链的区块并记录到分布式账本为止的处理。

[0040] 图3是以图1所示的区块链的区块生成间隔进行的处理的说明图。另外，在图3中，将事务数据表述为Tx数据，将事务池表述为Tx池。在图3中，区块生成间隔是例如从在区块链的区块B0上连接区块B1起到连接下一个区块B2为止的间隔。

[0041] 事务池是积存有区块链的还没有被验证的交易(事务数据)的储存库。如图3所示，在事务池中，从1个以上的用户取得的多个事务数据以未被验证的状态被保持。

[0042] 共识算法是用来选择向区块链写入区块的“代表者”的规则，也被称作共识形成算法。由于共识算法的执行需要时间，所以区块生成间隔由共识算法的执行开始起到执行完成为止的时间规定。

[0043] 对于到开始执行为止在事务池中选择的1个以上的事务数据，执行共识算法。如果共识算法的执行完成，则该区块被写入到区块链。另外，如果有能够包含保持于事务池中的全部事务数据的区块的容量，则也可以对保持于事务池中的全部的事务数据执行共识算法。

[0044] 图4是表示通过执行图3所示的共识算法而进行的处理的流程图的一例。

[0045] 如果执行共识算法，则首先进行在事务池中选择的1个以上的事务数据的验证(S91)。这里，进行该1个以上的事务数据的正当性的验证。

[0046] 接着，生成包含该1个以上的事务数据的区块(S92)，向区块链写入(S93)。另外，以下有将新的区块写入区块链的处理表现为将新的区块记录到分布式账本的情况。

[0047] 像这样，区块生成间隔由共识算法的执行所需要的时间规定。另外，在非专利文献1所公开的比特币中，共识算法的执行需要约10分钟，所以区块生成间隔被设为约10分钟。

[0048] 此外，在这样的区块链中，写入在保持为了向区块链写入而发送的事务数据的事务池中选择的事务数据。

[0049] 另外，在这样的区块链中，根据区块生成间隔，由相同的用户或相同的厂商在多个时间点发送的多个事务数据被保持于事务池。即，有由相同的用户或相同的厂商在多个时间点发送的多个事务数据被包含于1个区块的情况。

[0050] 但是，根据事务数据中包含的信息的种类，有即使在1个区块中包含由相同的用户

或相同的厂商在多个时间点发送的多个事务数据也没有意义的情况。在这样的情况下，在区块链的区块中会记录不利用的无用的事务数据。这不仅成为有限的网络带宽的浪费使用，也成为包括区块生成的电力等的资源的浪费使用。

[0051] 所以，有关本公开的一技术方案的控制方法，是在具备设备和多个服务器的系统中由上述设备执行的控制方法，所述多个服务器分别与上述设备可通信地连接，并按每规定的定时，将在到该规定的定时为止保持的事务数据中选择的事务数据包含于区块中并记录到分布式账本，在该控制方法中，生成包含到第1时间为止取得的最新信息的第1事务数据，发送给上述多个服务器中的第1服务器，在比上述第1时间靠后的1个以上的第2时间，通过确认记录在上述第1服务器的上述分布式账本中的区块的内容，来确认在上述第2时间生成了上述第1事务数据的后一个的第2事务数据时，上述第1事务数据被记录到上述分布式账本中时被包含于的第1区块与上述第2事务数据被记录到上述分布式账本中时被包含于的第2区块是否不同，在上述第1区块与上述第2区块不同的情况下，在该第2时间以后生成包含比上述第1时间靠后取得的最新信息的上述第2事务数据，发送给上述第1服务器。

[0052] 像这样，在确认记录在分布式账本中的区块的内容后，1个设备即相同的用户或相同的厂商发送包含最新信息的1个事务数据。由此，在向分布式账本记录的1个区块中会仅包含1个设备发送的1个事务数据。因此，能够抑制不利用的无用的事务数据记录到区块中，所以能够抑制网络带宽及资源的浪费使用。

[0053] 此外，也可以是，在确认上述区块的内容时，确认作为上述区块的内容，在上述区块中是否包含有在上述第1事务数据的前一个生成的第3事务数据。

[0054] 由此，在向分布式账本记录的每个区块中会仅包含1个设备发送的1个事务数据。因此，不仅能够抑制在区块中包含不被利用的事务数据并记录到分布式账本中，而且能够抑制对于该设备而言的空白区块记录到分布式账本中。因此，能够进一步抑制网络带宽及资源的浪费使用。

[0055] 这里，也可以是，还取得上述第1服务器每单位时间接收的事务数据数即接收总数、以及上述第1服务器向上述分布式账本记录时每单位时间能够处理的事务数据数即可处理数，在上述可处理数为根据上述接收总数设定的阈值以上的情况下，确认作为上述区块的内容，在上述区块中是否包含有上述第3事务数据。

[0056] 由此，能够根据第1服务器的处理能力，使得在向分布式账本记录的每个区块中仅包含1个设备发送的1个事务数据。

[0057] 此外，也可以是，在确认上述区块的内容时，确认作为上述区块的内容，在上述区块中是否包含有上述第1事务数据。

[0058] 由此，虽然发生对于该1个设备而言的空白区块被记录到分布式账本中的情况，但在向分布式账本记录的不是空白区块的1个区块中会仅包含由1个设备发送的1个事务数据。因此，能够抑制不利用的无用的事务数据被记录到区块中，所以能够抑制网络带宽及资源的浪费使用。

[0059] 这里，也可以是，还取得上述第1服务器每单位时间接收的事务数据数即接收总数、以及上述第1服务器向上述分布式账本记录时每单位时间能够处理的事务数据数即可处理数，在上述可处理数比根据上述接收总数设定的阈值小的情况下，确认作为上述区块的内容，在上述区块中是否包含有上述第1事务数据。

[0060] 由此，根据第1服务器的处理能力，能够使得在向分布式账本记录的1个区块中仅包含由1个设备发送的1个事务数据。

[0061] 此外，有关本公开的一技术方案的数据生成装置，与多个服务器可通信地连接，所述多个服务器分别按每规定的定时，将在到该规定的定时为止保持的事务数据中选择的事务数据包含于区块中并记录到分布式账本，上述数据生成装置具备：处理器；以及存储器，上述处理器生成包含到第1时间为止取得的最新信息的第1事务数据，发送给上述多个服务器中的第1服务器；上述处理器在比上述第1时间靠后的1个以上的第2时间，通过确认记录在上述第1服务器的上述分布式账本中的区块的内容，来确认在上述第2时间生成了上述第1事务数据的后一个的第2事务数据时，上述第1事务数据被记录到上述分布式账本中时被包含于的第1区块与上述第2事务数据被记录到上述分布式账本中时被包含于的第2区块是否不同，上述处理器在确认到上述第1区块与上述第2区块不同的情况下，在该第2时间以后生成包含比上述第1时间靠后取得的最新信息的上述第2事务数据，发送给上述第1服务器。

[0062] 以下，参照附图对实施方式进行说明。另外，以下说明的实施方式都表示本公开的优选的一具体例。即，在以下的实施方式中表示的数值、形状、材料、构成要素、构成要素的配置及连接形态、步骤、步骤的顺序等是一例，不是限定本公开的意思。本公开基于权利要求书的记载而确定。因而，以下的实施方式的构成要素中的、在表示本公开的最上位概念的独立权利要求中没有记载的构成要素，虽然不是为了达成本公开的课题而必定需要的，但作为构成更优选的形态的构成要素而进行说明。

[0063] (实施方式)

[0064] 以下，参照附图对有关实施方式的控制系统进行说明。

[0065] 在本公开的控制系统中，根据对向最新的分布式账本记录的区块的内容进行了确认的结果，发送下一个事务数据。由此，在虽然想要定期地向分布式账本记录信息，但想要不参照记录在分布式账本中的过去的信息而仅利用最新信息的情况下，在向分布式账本记录的1个区块中会仅包含：包含可能被利用的最新信息的1个事务数据。

[0066] [控制系统的构成]

[0067] 图5是示意地表示有关本实施方式的控制系统的构成的图。

[0068] 如图5所示，控制系统具备设备100和认证服务器装置210、220、230。它们可通信地连接。这些通信只要是有线的因特网线、无线通信及专用通信等的某种即可。

[0069] 另外，在图5中表示了有关本实施方式的控制系统具备3个服务器和1个设备的情况下的例子，但并不限于此。即，有关本实施方式的控制系统也可以具备4个以上的认证服务器装置，也可以具备两个以上的设备。另外，1个设备代表一个用户或一个厂商所利用的设备，也可以是具有服务器功能的设备，在后面叙述。

[0070] [设备100]

[0071] 设备100代表一个用户或一个厂商所利用的设备。设备100也可以具有服务器功能。

[0072] 图6是示意地表示有关本实施方式的设备100的构成的框图。

[0073] 设备100具备处理器和存储有使处理器执行规定的处理的程序的存储器。即，设备100通过由处理器使用存储器执行规定的程序来实现。在本实施方式中，设备100具备传感器信息取得部101、事务数据生成部102、事务数据确认部103、确认方法决定部104和通信部

105。另外，确认方法决定部104不是必须的构成，设备100也可以不具备确认方法决定部104。以下，对各构成要素进行说明。

[0074] 〈传感器信息取得部101〉

[0075] 传感器信息取得部101定期地取得来自搭载于未图示的IoT(Internet of Things)设备的传感器的信息(传感器信息)。即，传感器信息取得部101定期地取得最新的传感器信息(以下，也称作最新信息)。这里，传感器信息例如是天气信息或生物体信息，但并不限于这些。传感器信息也可以是从传感器直接取得的数据，例如也可以是经由因特网从传感器取得的数据。此外，传感器信息也可以是从因特网上取得的数据、并且是被定期地更新或追加的数据。

[0076] 〈事务数据生成部102〉

[0077] 事务数据生成部102基于事务数据确认部103的确认结果生成事务数据。事务数据生成部102将所生成的事务数据经由通信部105发送给认证服务器装置210、220、230的至少1个。

[0078] 更具体地讲，假设事务数据生成部102生成包含到第1时间为止由传感器信息取得部101取得的最新信息的第1事务数据，将所生成的第1事务数据例如发送给认证服务器装置210。在此情况下，事务数据生成部102根据由事务数据确认部103确认的记录在最新的分布式账本中的区块的内容，生成包含比第1时间靠后取得的最新信息的第2事务数据。并且，事务数据生成部102将所生成的第2事务数据发送给认证服务器装置210。

[0079] 〈事务数据确认部103〉

[0080] 事务数据确认部103确认在记录于最新的分布式账本的区块中，是否包含有事务数据生成部102在前一个或两个之前生成并发送的事务数据。通过确认记录在最新的分布式账本中的区块的内容，能够确认是否到了将事务数据生成部102接下来生成的事务数据记录到与之前生成的事务数据不同的区块中的定时。

[0081] 更具体地讲，事务数据确认部103在比第1时间靠后的1个以上的第2时间，通过确认被记录在分布式账本中的区块的内容，来确认第1区块和第2区块是否不同。

[0082] 这里，将第1事务数据被记录到分布式账本中时被包含于的区块称作第1区块。将在第2时间生成了第1事务数据的后1个的第2事务数据时，第2事务数据被记录到分布式账本中时被包含于的区块称作第2区块。

[0083] 并且，事务数据确认部103在确认到第1区块和第2区块不同的情况下，使事务数据生成部102在该第2时间以后生成包含比第1时间靠后取得的最新信息的第2事务数据。

[0084] 这里，事务数据确认部103也可以确认作为记录在最新的分布式账本中的区块的内容，例如在该区块中是否包含有第1事务数据的前一个生成的第3事务数据。并且，事务数据确认部103只要确认到在该区块中包含有第3事务数据，就使事务数据生成部102生成第2事务数据即可。由此，被记录到分布式账本中的每个区块中会仅包含设备100生成的1个第2事务数据。

[0085] 此外，事务数据确认部103也可以确认作为记录在最新的分布式账本中的区块的内容，例如在该区块中是否包含有第1事务数据。并且，事务数据确认部103只要确认到在该区块中包含有第1事务数据，就使事务数据生成部102生成第2事务数据即可。由此，尽管发生不包含第2事务数据的空白区块被记录到分布式账本中的情况，但被记录到分布式账本

中的不是空白区块的1个区块中会仅包含设备100生成的1个第2事务数据。

[0086] 〈确认方法决定部104〉

[0087] 确认方法决定部104也可以根据认证服务器装置210的处理能力，决定事务数据确认部103进行的记录在最新的分布式账本中的区块的内容的确认方法。

[0088] 更具体地讲，确认方法决定部104取得第1服务器每单位时间接收的事务数据数即接收总数、以及第1服务器在向分布式账本记录时每单位时间能够处理的事务数据数即可处理数。

[0089] 确认方法决定部104也可以在可处理数为根据接收总数决定的阈值以上的情况下，使事务数据确认部103确认作为记录在最新的分布式账本中的区块的内容，在区块中是否包含有第3事务数据。

[0090] 此外，确认方法决定部104也可以在可处理数比根据接收总数决定的阈值小的情况下，使事务数据确认部103确认作为记录在最新的分布式账本中的区块的内容，在区块中是否包含有第1事务数据。

[0091] 通过这些，确认方法决定部104能够使事务数据确认部103确认在记录在最新的分布式账本中的区块中是否包含有事务数据生成部102在前一个或两个之前生成并发送的事务数据。

[0092] 另外，关于从包括设备100的多个设备发送的事务数据的数量，如果向认证服务器装置210等确认，则即使不是正确的数量也可以大体取得能够进行上述的确认的程度。此外，每单位时间能够处理的事务数据数由认证服务器装置210等分别预先决定。

[0093] 〈通信部105〉

[0094] 通信部105进行与认证服务器装置210、220、230的通信。

[0095] 在本实施方式中，通信部105将由事务数据生成部102生成的事务数据发送给认证服务器装置210、220、230的至少1个。此外，通信部105也可以作为认证服务器装置210、220、230的处理能力而取得接收总数和可处理数，并发送给确认方法决定部104。此外，通信部105也可以取得认证服务器装置210、220、230的最新的分布式账本的内容，并发送给事务数据确认部103。

[0096] [设备100的硬件构成]

[0097] 接着，使用图7对有关本实施方式的设备100的硬件构成进行说明。图7是表示通过软件实现有关本实施方式的设备100的功能的计算机1000的硬件构成的一例的图。

[0098] 如图7所示，计算机1000是具备输入装置1001、输出装置1002、CPU1003、内置存储设备1004、RAM1005、读取装置1007、收发装置1008及总线1009的计算机。输入装置1001、输出装置1002、CPU1003、内置存储设备1004、RAM1005、读取装置1007及收发装置1008通过总线1009连接。

[0099] 输入装置1001是输入按钮、触摸板、触控面板显示器等的作为用户接口的装置，受理用户的操作。另外，输入装置1001也可以是除了受理用户的接触操作之外还受理通过声音的操作、通过遥控器等的远程操作的构成。

[0100] 内置存储设备1004是闪存存储器等。此外，内置存储设备1004也可以预先存储用来实现设备100的功能的程序及利用设备100的功能构成的应用的至少一方。

[0101] RAM1005是随机访问存储器(Random Access Memory)，在执行程序或应用时利用

于数据等的存储。

[0102] 读取装置1007从USB(Universal Serial Bus)存储器等的记录介质读取信息。读取装置1007从记录有如上所述的程序或应用的记录介质读取该程序或应用,使内置存储设备1004存储。

[0103] 收发装置1008是用来以无线或有线方式进行通信的通信电路。收发装置1008例如与连接在网络上的服务器装置进行通信,从服务器装置下载如上所述的程序或应用,使内置存储设备1004存储。

[0104] CPU1003是中央运算处理装置(Central Processing Unit),将存储在内置存储设备1004中的程序、应用复制到RAM1005中,将该程序或应用中包含的命令从RAM1005依次读出并执行。

[0105] 接着,对认证服务器装置210进行说明。

[0106] [认证服务器装置210]

[0107] 由于认证服务器装置210、220及230是同样的构成,所以以认证服务器装置210为例进行说明。

[0108] 图8是表示有关本实施方式的认证服务器装置210的功能构成的框图。

[0109] 认证服务器装置210与设备100可通信地连接,按每规定的定时将在到该规定的定时为止所保持的事务数据中选择的事务数据包含于区块中,并记录到分布式账本。认证服务器装置210是向分布式账本进行记录的第1服务器的一例。

[0110] 在本实施方式中,如图8所示,认证服务器装置210具备事务数据保存部211、事务数据验证部212、账本保存部213和通信部214。认证服务器装置210可以通过由处理器使用存储器执行规定的程序来实现。以下,对各构成要素进行说明。

[0111] <事务数据保存部211>

[0112] 事务数据保存部211作为积存有区块链的还没有被验证的事务数据的事务池发挥功能。

[0113] 在本实施方式中,事务数据保存部211保存从设备100取得的例如第1事务数据、第2事务数据或第3事务数据,并暂时地保持。事务数据保存部211在所保持的事务数据中,删除被选择并被写入到分布式账本的事务数据,或丢弃不再需要的事务数据。

[0114] 另外,事务数据保存部211也可以在从设备100取得了事务数据时,进行该事务数据中包含的电子签名的验证和事务数据的正当性的验证。并且,事务数据保存部211也可以仅在从设备100取得的事务数据的验证成功的情况下保持从设备100取得的事务数据。另外,也可以将该验证跳过。

[0115] <事务数据验证部212>

[0116] 事务数据验证部212通过执行共识算法,对从保持在事务数据保存部211中的事务数据中选择的事务数据的正当性进行验证。

[0117] 这里,在共识算法中,既可以使用PBFT(Practical Byzantine Fault Tolerance:实用拜占庭容错算法),也可以使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:工作量证明)或POS(Proof Of Stake:权益证明)等。在共识算法中使用PBFT的情况下,事务数据验证部212从其他多个认证服务器装置220及230分别接受表示事务数据的验证是否成功的报告,判定该报告的数量是否超过了规定的数量。并且,事务数

据验证部212在该报告的数量超过了规定的数量时判定为通过共识算法验证了事务数据的正当性即可。

[0118] 〈账本保存部213〉

[0119] 账本保存部213是将应向分布式账本保存的新的事务数据向分布式账本保存的处理部。

[0120] 在本实施方式中，账本保存部213生成包含由事务数据验证部212验证了正当性的事务数据的区块，将所生成的区块记录到分布式账本中。换言之，账本保存部213生成包含由事务数据验证部212验证了正当性的事务数据的区块，写入到保存在分布式账本中的区块链。

[0121] 〈通信部214〉

[0122] 通信部214进行与认证服务器装置220、230的通信，或进行与设备100的通信。

[0123] 在本实施方式中，通信部214将事务数据验证部212的验证对象的事务数据发送给认证服务器装置220及230。此外，通信部214也可以与设备100进行通信，取得事务数据，或作为认证服务器装置210自身的处理能力而将接收总数和可处理数发送给设备100。此外，通信部214也可以将认证服务器装置210自身所具有的分布式账本的内容发送给设备100。

[0124] [动作]

[0125] 接着，对如以上那样构成的控制系统中包含的设备100的动作进行说明。

[0126] 图9是表示有关本实施方式的设备100的动作的流程图。

[0127] 在图9中表示了使得在向分布式账本记录的1个区块所包含的1个以上的事务数据之中，对于设备100而言仅包含设备100发送的1个事务数据的动作。

[0128] 首先，设备100生成包含到第1时间为止取得的最新信息的第1事务数据，发送给第1服务器(S10)。如上所述，第1服务器例如相当于认证服务器装置210。

[0129] 接着，设备100在比第1时间靠后的第2时间，确认记录在第1服务器的分布式账本中的区块的内容(S11)。更具体地讲，设备100确认记录在分布式账本中的区块的内容，确认在第2时间生成了第1事务数据的后1个的第2事务数据时是否被包含于与第1事务数据不同的区块中。

[0130] 接着，设备100当在第2时间生成了第2事务数据的情况下被包含于与第1事务数据不同的区块中的情况下(S12中是)，生成包含比第1时间靠后取得的最新信息的第2事务数据，发送给第1服务器(S13)。在本实施方式中，从第2时间以后到在第2时间时间点执行的共识算法的执行完成为止，设备100生成第2事务数据，发送给第1服务器。

[0131] 另外，设备100当在第2时间生成了第2事务数据时被包含于与第1事务数据相同的区块中的情况下(S12中否)，回到步骤S11，重新进行处理。

[0132] (实施例1)

[0133] 接着，作为实施例1，说明如下情况下的控制系统的处理：设备100确认作为区块的内容，在记录于最新的分布式账本中的区块中是否包含有设备100自身在两个之前发送的事务数据。

[0134] 图10是有关实施例1的控制系统的处理的顺序图。在图10中表示图9所示的S11以后的控制系统的处理的一例。

[0135] 这里，假设设备100生成包含到第1时间为止取得的最新信息的第1事务数据并发

送给认证服务器装置210、220、230，由认证服务器装置210、220、230至少将第1事务数据入池(保存)。

[0136] 接着，在比第1时间靠后的第2时间，设备100确认认证服务器装置210的最新的分布式账本(S21)。在本实施例中，设备100例如对认证服务器装置210请求最新的分布式账本，通过取得由认证服务器装置210发送的最新的分布式账本，确认最新的分布式账本。

[0137] 接着，设备100参照(确认)所取得的最新的分布式账本的区块，确认是否包含有设备100自身在两个之前发送的第3事务数据(S22)。这里，将设备100在前一个发送的事务数据设为第1事务数据。此外，将设备100在两个之前发送的即在第1事务数据的前一个发送的事务数据设为第3事务数据。换言之，以设备100以后(即第2时间以后)生成并发送的第2事务数据为基准，将前一个发送的事务数据称作第1事务数据。此外，以设备100以后发送的第2事务数据为基准，将两个之前发送的事务数据称作第3事务数据。

[0138] 在步骤S22中，设备100在最新的分布式账本中包含有设备100自身在两个之前发送的第3事务数据的情况下(S22中是)，生成包含比第1时间靠后取得的最新信息的第2事务数据(S23)。另外，在步骤S22中，设备100在最新的分布式账本中没有包含设备100自身在两个之前发送的第3事务数据的情况下(S22中否)，回到步骤S21，重新进行处理。

[0139] 接着，设备100将在步骤S23中生成的第2事务数据发送给认证服务器装置210、220、230(S24)。

[0140] 于是，认证服务器装置210、220、230分别将从设备100取得的第2事务数据入池(保存)(S25)。

[0141] (实施例2)

[0142] 接着，作为实施例2，说明设备100根据认证服务器装置210的处理能力决定记录在认证服务器装置210的最新的分布式账本中的区块的内容的确认方法的情况下的处理。此外，在本实施例中，假设区块的内容的确认方法是确认在记录在最新的分布式账本中的区块中是否包含有设备100自身在两个之前或前一个发送的事务数据的方法而进行说明。

[0143] 图11是表示有关实施例2的设备100的处理的流程图。

[0144] 假设设备100在进行以下说明的步骤S31之前，生成包含到第1时间为止取得的最新信息的第1事务数据，发送给认证服务器装置210，由认证服务器装置210至少将第1事务数据入池(保存)。

[0145] 首先，设备100从认证服务器装置210取得认证服务器装置210的每单位时间的可处理数和接收总数(S31)。

[0146] 接着，设备100确认在步骤S31中取得的可处理数是否为阈值以上(即，可处理数≥阈值)(S32)。关于这里的阈值，根据设备100在步骤S31中取得的接收总数来设定，例如设定为接收总数的百分之几至百分之十几左右的值。

[0147] 在步骤S32中，在可处理数比阈值小的情况下(S32中否)，在比第1时间靠后的第2时间，设备100确认认证服务器装置210的最新的分布式账本(S33)。在本实施例中，设备100也例如向认证服务器装置210请求最新的分布式账本，取得由认证服务器装置210发送的最新的分布式账本，从而确认最新的分布式账本。

[0148] 另一方面，在步骤S32中，在可处理数为阈值以上的情况下(S32中是)，向步骤S33前进。以后的处理即步骤S33、步骤S35及步骤S36的处理如在图10的步骤S21～步骤S24中说

明的那样，所以省略说明。

[0149] 另外，设为设备100在步骤S31之前生成包含最新信息的第1事务数据并发送给认证服务器装置210而进行了说明，但并不限于此。也可以在步骤S31及S32之后并且步骤S33之前生成包含最新信息的第1事务数据并发送给认证服务器装置210。

[0150] [效果等]

[0151] 以上，根据有关实施方式的控制系统等，确认记录在分布式账本中的区块的内容后，1个设备100即相同的用户或相同的厂商发送包含最新信息的1个事务数据。换言之，在有关实施方式的控制系统等中，设备100将事务数据不是以PUSH型发送，而是以ASK型一个个地发送。由此，在记录于分布式账本的1个区块中，对于设备100而言仅包含1个设备100发送的1个事务数据。因此，能够抑制不利用的无用的事务数据记录于区块中，所以能够抑制网络带宽及资源的浪费使用。

[0152] 这里，使用图12～图14对有关实施方式的效果进行说明。图12及图13是用来对有关实施方式的效果进行说明的流程图。图14是图13所示的流程图的其他观点下的说明图。

[0153] 首先，使用图12，说明设备100在确认以预计接下来生成的第2事务数据为基准而前一个生成的第1事务数据包含于记录在最新的分布式账本中的区块的情况之后，生成并发送第2事务数据的情况。

[0154] 在图12中，将第1事务数据表述为Tx_{n-1}，将第2事务数据表述为Tx_n。此外，将执行共识算法的期间表述为共识。执行共识算法的期间被表示为为了向区块链写入区块所需要的期间。在图12所示的区块链中，表示了对于到共识算法的开始前为止所发送的事务数据执行共识算法，在共识算法的执行完成后包含于区块中并向区块链写入。到共识算法的开始前为止所发送的事务数据被保持在事务池中。

[0155] 如图12所示，设备100也可以定期地确认在生成后发送的Tx_{n-1}是否包含于被写入到区块链的区块中。在此情况下，设备100如果确认到在被写入到区块链的区块中包含有Tx_{n-1}，则生成并发送Tx_n。于是，在连续的区块各自中不包含设备100生成并发送的事务数据(发生对于设备100而言的空白区块)。但是，在不是空白区块的区块中，对于设备100而言会仅包含设备100生成并发送的1个事务数据。

[0156] 即，设备100也可以在确认在被写入到区块链的区块中包含有设备100在前一个发送的事务数据之后发送下一个事务数据。由此，设备100能够抑制尽管有在被写入到区块链的区块中发生对于设备100而言的空白区块的情况、但设备100发送的两个以上的事务数据被包含在1个区块中。

[0157] 像这样，虽然发生对于设备100而言空白区块被记录到分布式账本中的情况，但在记录于分布式账本的1个区块中，对于设备100而言会仅包含由设备100发送的1个事务数据。

[0158] 因此，能够抑制不利用的无用的事务数据被记录到区块中，所以能够抑制网络带宽及资源的浪费使用。

[0159] 接着，使用图13及图14，说明设备100在确认以预计接下来生成的第2事务数据为基准而在两个之前生成的第3事务数据包含在记录于最新的分布式账本的区块中之后生成并发送第2事务数据的情况。这里，在图13及图14中，第1事务数据是以预计接下来生成的第2事务数据为基准在前一个生成的事务数据，表述为Tx_{n-1}。此外，将第2事务数据表述为Tx_n，

将在第1事务数据的前一个生成的第3事务数据表述为Tx_{n-2}。此外，将预计在第2事务数据的后一个生成的事务数据表述为Tx_{n+1}。

[0160] 如图13及图14所示，设备100为了确认Tx_n的生成及发送定时，在Tx_{n-1}的发送后，确认Tx_{n-2}是否包含于被写入到区块链的区块中。并且，也可以是，设备100如果确认到在被写入到区块链的区块中包含有Tx_{n-2}，则生成并发送Tx_n。

[0161] 接着，设备100为了确认Tx_{n+1}的生成及发送定时，在Tx_n的发送后，确认Tx_{n-1}是否包含于被写入到区块链的区块中。并且，设备100如果确认到在被写入到区块链的区块中包含有Tx_{n-1}，则生成并发送Tx_{n+1}。因此，在连续的区块各自中会包含设备100生成并发送的事务数据(不发生对于设备100而言的空白区块)。

[0162] 像这样，设备100在确认在被写入到区块链的区块中包含有设备100在两个之前发送的事务数据之后发送下一个事务数据。由此，在1个区块中，对于设备100而言会仅包含设备100生成并发送的1个事务数据。即，能够抑制设备100发送的两个以上的事务数据包含于1个区块中。此外，在每个区块中对于设备100而言仅包含设备100生成并发送的1个事务数据，所以也能够抑制对于设备100而言发生空白区块。

[0163] 换言之，不仅能够抑制不被利用的1个以上的事务数据被包含在区块中而被记录到分布式账本，还能够抑制对于该设备而言的空白区块被记录到分布式账本。因此，能够进一步抑制网络带宽及资源的浪费使用。

[0164] 此外，也可以根据具有分布式账本的认证服务器装置的处理能力，确认在记录于最新的分布式账本的区块中包含有第1事务数据的情况，或包含有在第1事务数据的前一个生成的第3事务数据的情况。由此，能够根据认证服务器装置的处理能力，选择是否容许发生对于设备100而言的空白区块被记录到分布式账本的情况。

[0165] [其他变形例]

[0166] 如以上这样，基于上述的实施方式对本公开进行了说明，但本公开当然并不限定于上述的实施方式。以下这样的情况也包含在本公开中。

[0167] (1)有关上述实施方式的各装置具体而言是由微处理器、ROM、RAM、SSD、硬盘单元、显示器单元、键盘、鼠标等构成的计算机系统。在上述RAM或硬盘单元中记录有计算机程序。通过由上述微处理器按照上述计算机程序动作，各装置达成其功能。这里，计算机程序是为了达成规定的功能而将多个表示对于计算机的指令的命令代码组合而构成的。

[0168] (2)构成上述实施方式的各装置的构成要素的一部分或全部也可以由1个系统LSI(Large Scale Integration:大规模集成电路)构成。系统LSI是将多个构成部集成到1个芯片上而制造出的超多功能LSI，具体而言，是包括微处理器、ROM、RAM等而构成的计算机系统。在上述RAM中记录有计算机程序。通过由上述微处理器按照上述计算机程序动作，系统LSI达成其功能。

[0169] 此外，构成上述各装置的构成要素的各部既可以单独地被单芯片化，也可以以包含一部分或者全部的方式被单芯片化。

[0170] 此外，这里设为系统LSI，但根据集成度的差异，有时也称为IC、LSI、超级LSI、特级LSI。另外，集成电路化的方法不限于LSI，也可以由专用电路或者通用处理器实现。也可以利用在LSI制造后能够编程的FPGA(Field Programmable Gate Array:现场可编程逻辑门阵列)或能够重构LSI内部的电路单元的连接或设定的可重构处理器。

[0171] 进而，如果因半导体技术的进步或派生的其他技术而出现替代LSI的集成电路化的技术，则当然也可以使用该技术进行功能块的集成化。有可能是生物技术的应用等。

[0172] (3)构成上述各装置的构成要素的一部分或全部也可以由相对于各装置可拆装的IC卡或单体的模块构成。上述IC卡或上述模块是由微处理器、ROM、RAM等构成的计算机系统。上述IC卡或上述模块也可以包括上述的超多功能LSI。通过由微处理器按照计算机程序动作，上述IC卡或上述模块达成其功能。该IC卡或该模块也可以具有耐篡改性。

[0173] (4)本公开也可以是上述所示的方法。此外，也可以是通过计算机实现这些方法的计算机程序，也可以是由上述计算机程序构成的数字信号。

[0174] 此外，本公开也可以将上述计算机程序或上述数字信号记录到能够由计算机读取的记录介质，例如软盘、硬盘、CD－ROM、MO、DVD、DVD－ROM、DVD－RAM、BD(Blu－ray(注册商标)Disc)、半导体存储器等中。此外，也可以是记录在这些记录介质中的上述数字信号。

[0175] 此外，本公开也可以将上述计算机程序或上述数字信号经由电气通信线路、无线或有线通信线路、以因特网为代表的网络、数据广播等传送。

[0176] 此外，本公开也可以是具备微处理器和存储器的计算机系统，上述存储器记录有上述计算机程序，上述微处理器按照上述计算机程序动作。

[0177] 此外，也可以通过将上述程序或上述数字信号记录到上述记录介质中并移送，或通过将上述程序或上述数字信号经由上述网络等移送，来由独立的其他的计算机系统实施。

[0178] (5)也可以将上述实施方式及上述变形例分别组合。

[0179] 工业实用性

[0180] 本公开能够利用于向分布式账本记录的事务数据的控制方法及数据生成装置，特别是能够利用于虽然将最新信息定期地记录到分布式账本、但仅利用最新信息而不利用过去的信息的向分布式账本记录的事务数据的控制方法及数据生成装置。

[0181] 标号说明

[0182] 100 设备

[0183] 101 传感器信息取得部

[0184] 102 事务数据生成部

[0185] 103 事务数据确认部

[0186] 104 确认方法决定部

[0187] 105、214 通信部

[0188] 210、220、230 认证服务器装置

[0189] 211 事务数据保存部

[0190] 212 事务数据验证部

[0191] 213 账本保存部

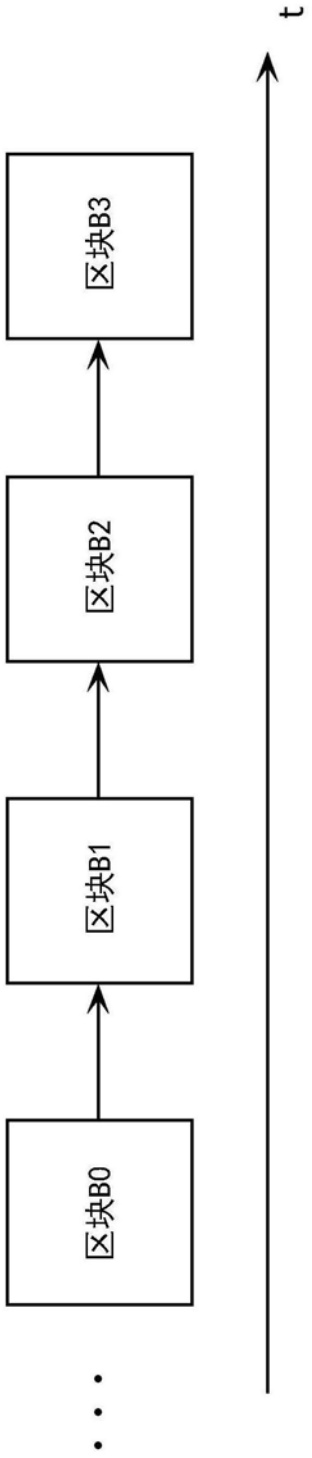


图1

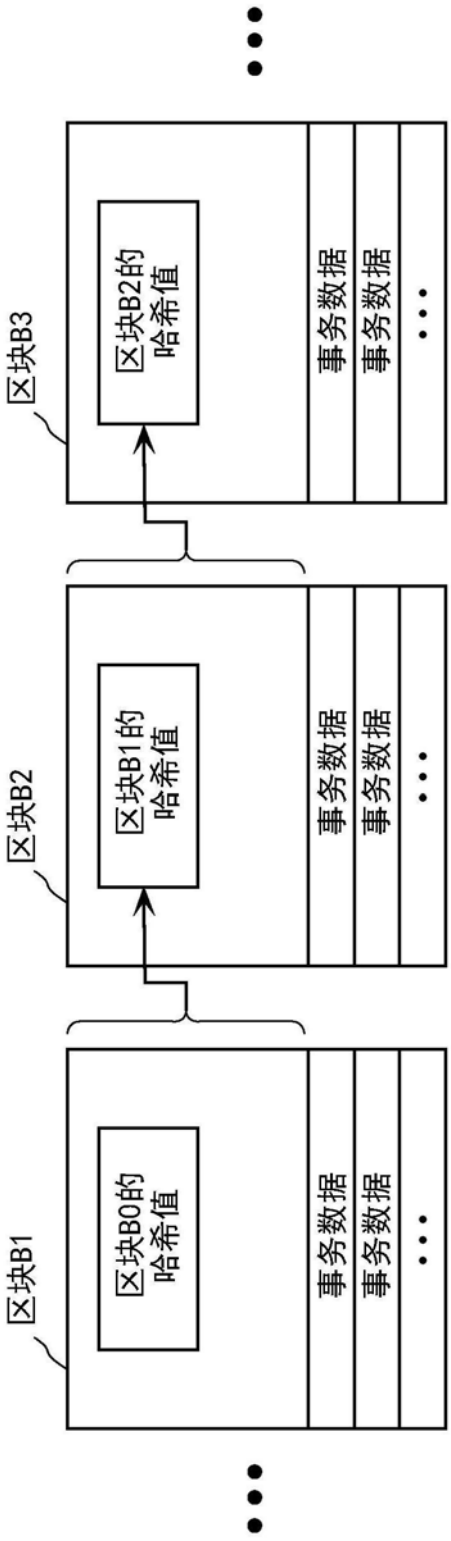

区块B3
区块B2的
哈希值
事务数据
事务数据
区块B2
区块B1的
哈希值
事务数据
事务数据
区块B1
区块B0的
哈希值
事务数据
事务数据

图2

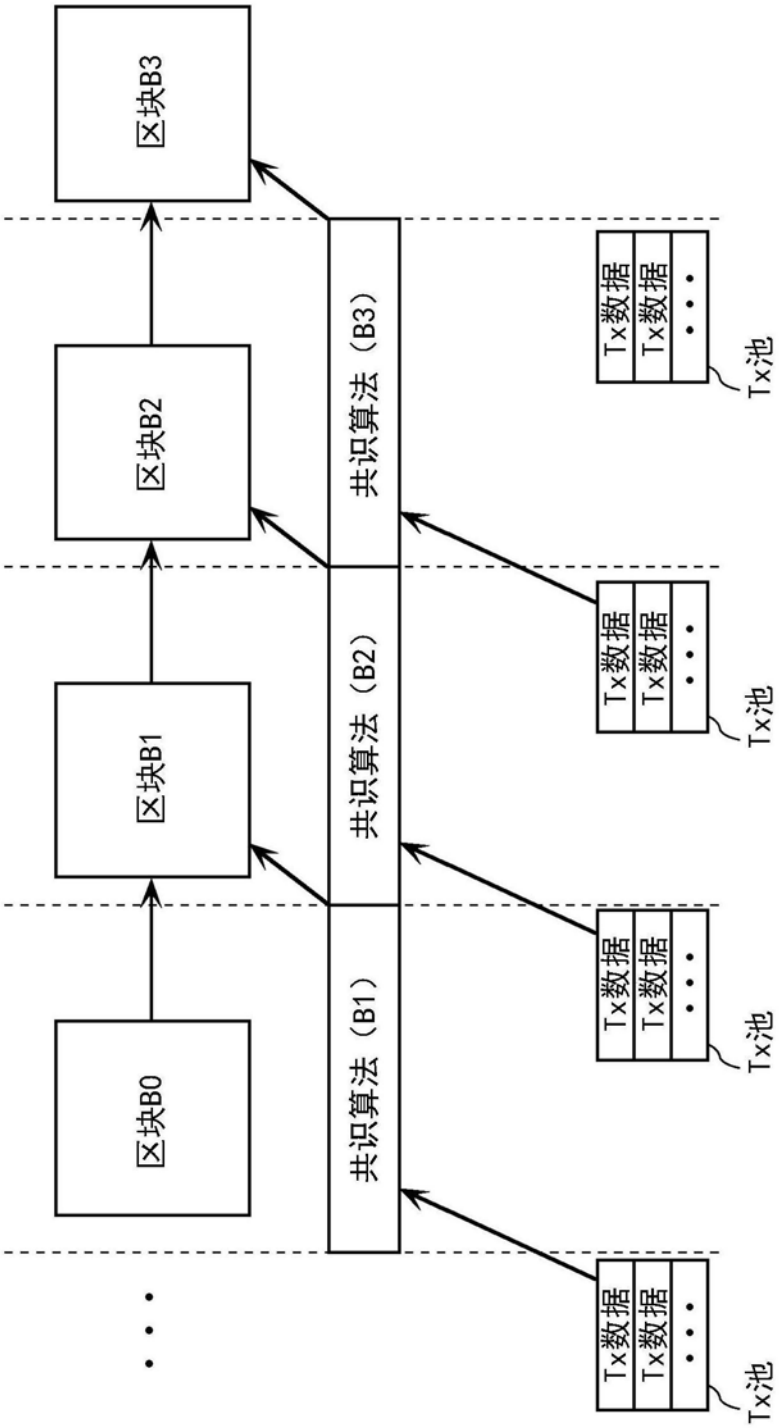


图3

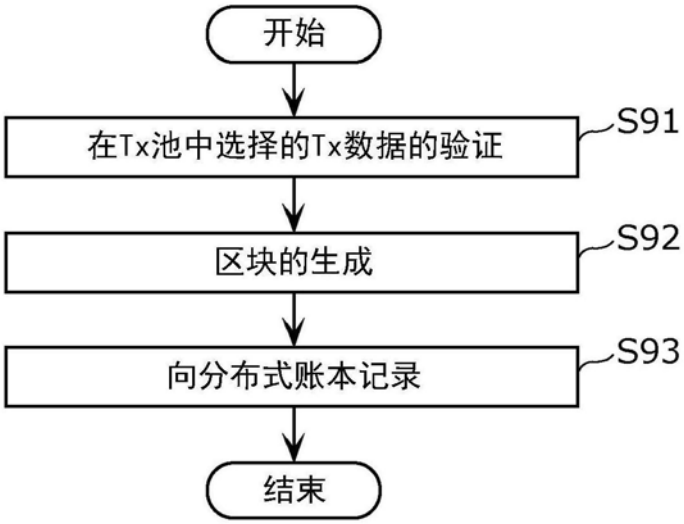

开始
在Tx池中选择的Tx数据的验证
S91
区块的生成
S92
向分布式账本记录
S93
结束

图4

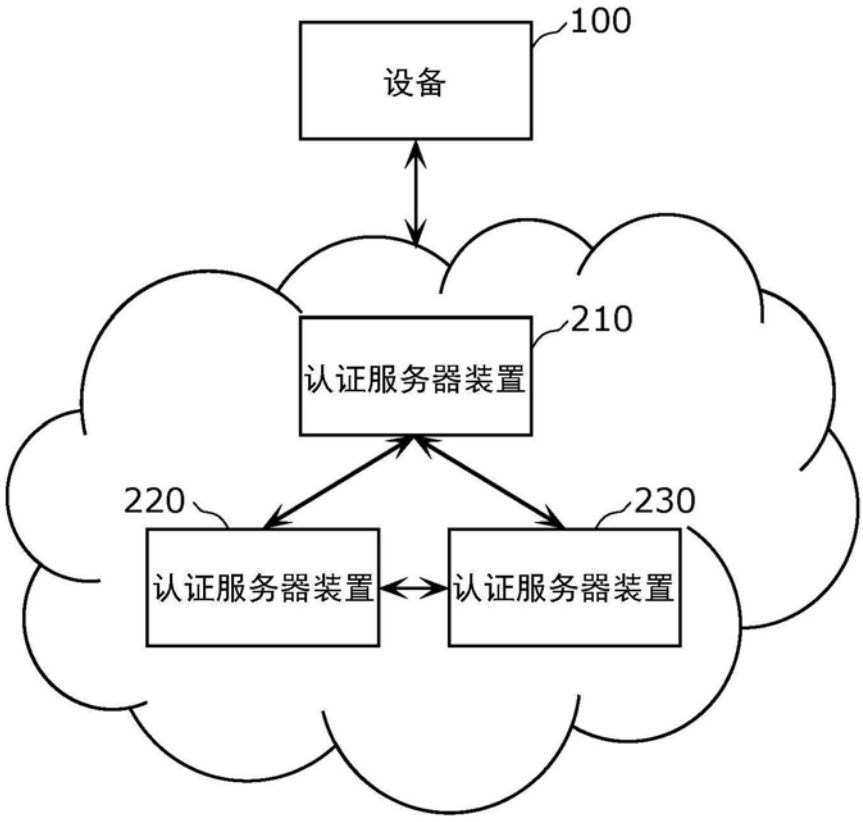

100
设备
210
认证服务器装置
220
230
认证服务器装置
认证服务器装置

图5

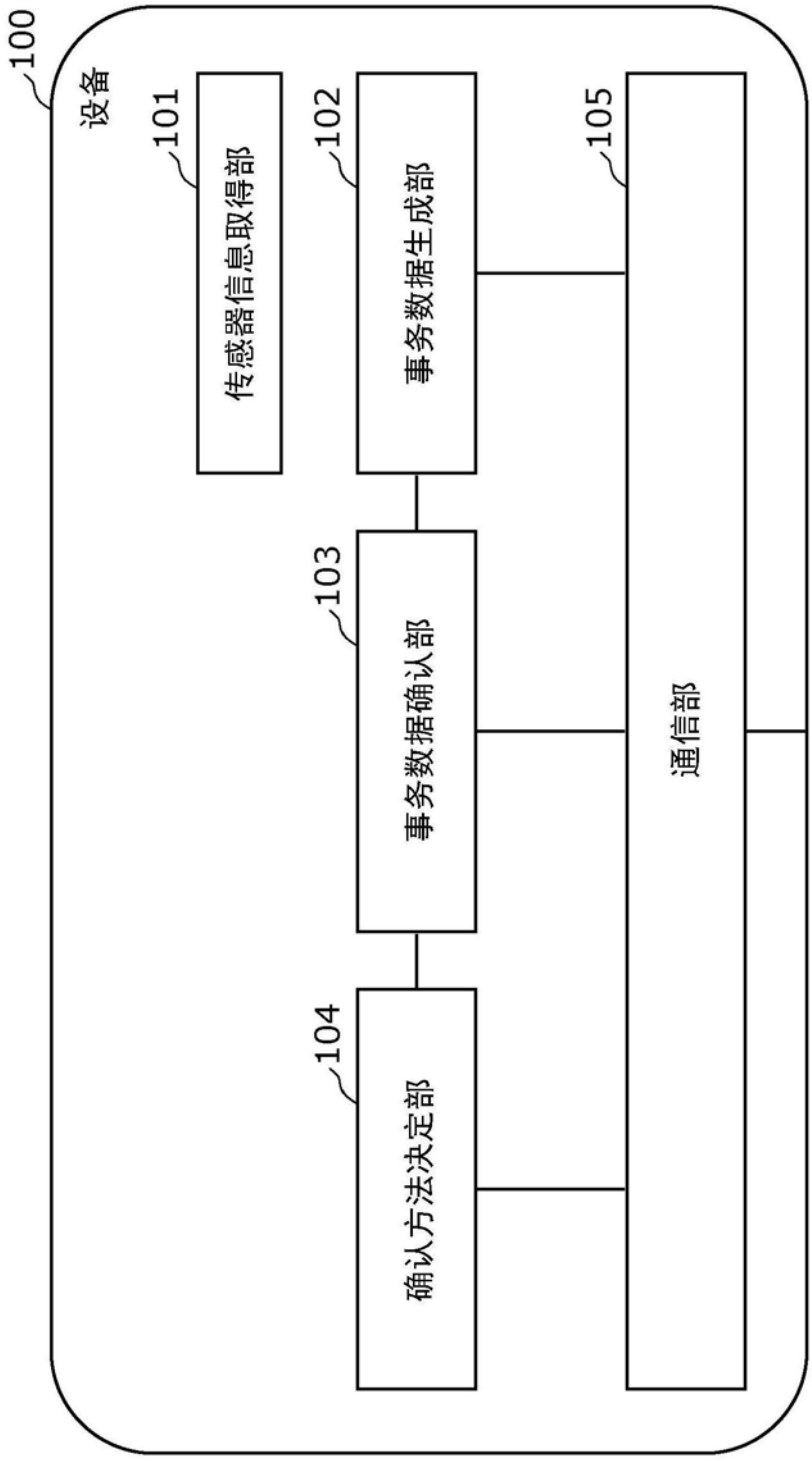

100
设备
101
传感器信息取得部
102
事务数据生成部
103
事务数据确认部
104
确认方法决定部
105
通信部

图6

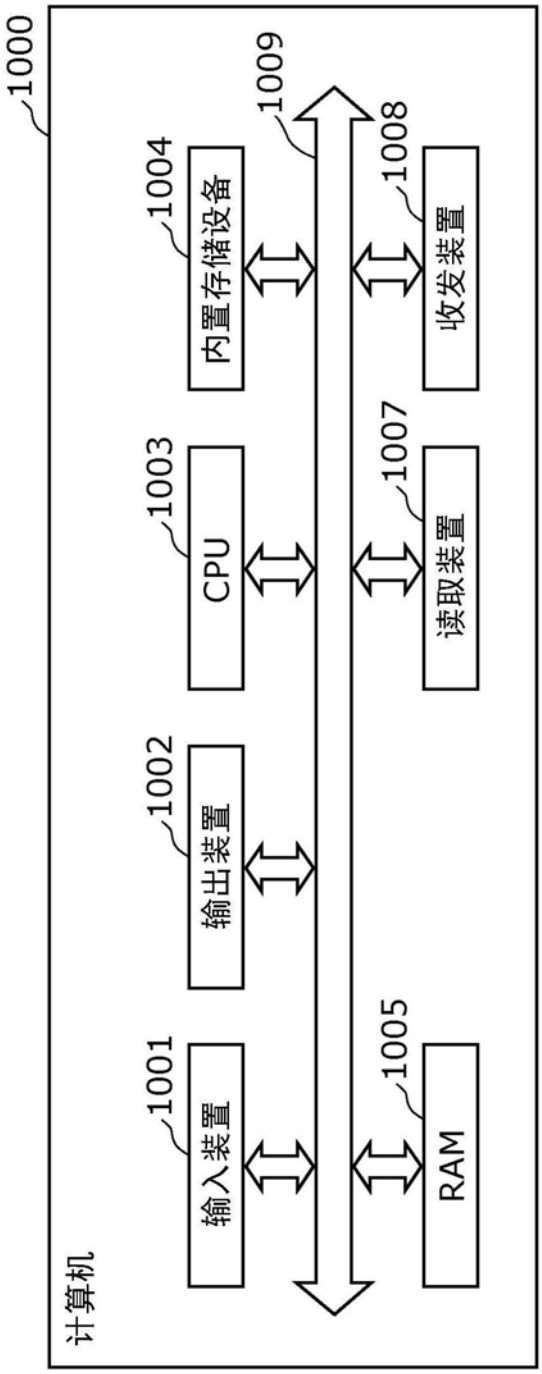

1000
计算机
1001
输入装置
1002
输出装置
1003
CPU
1004
内置存储设备
1005
RAM
1007
读取装置
1008
收发装置
1009

图7

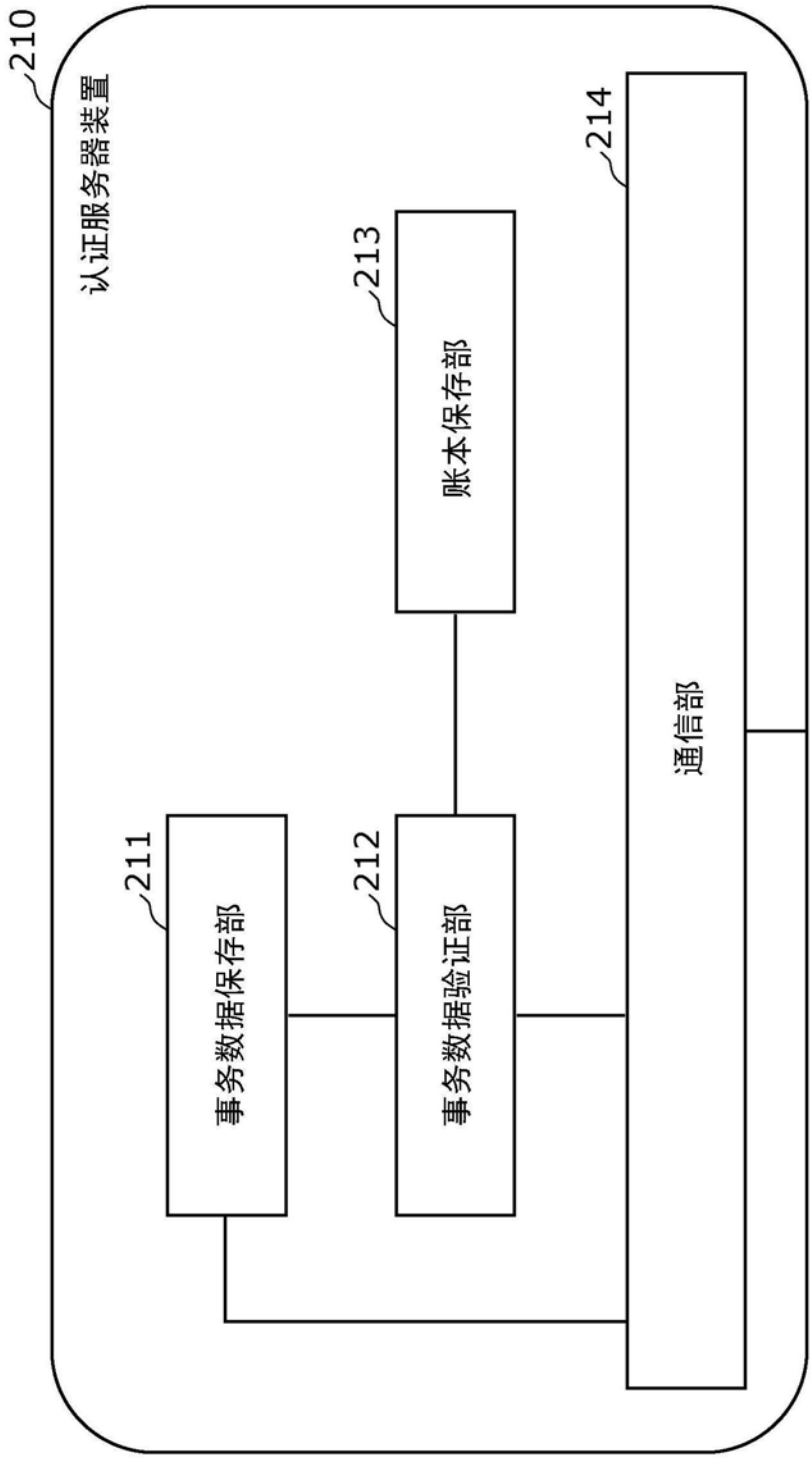


图8

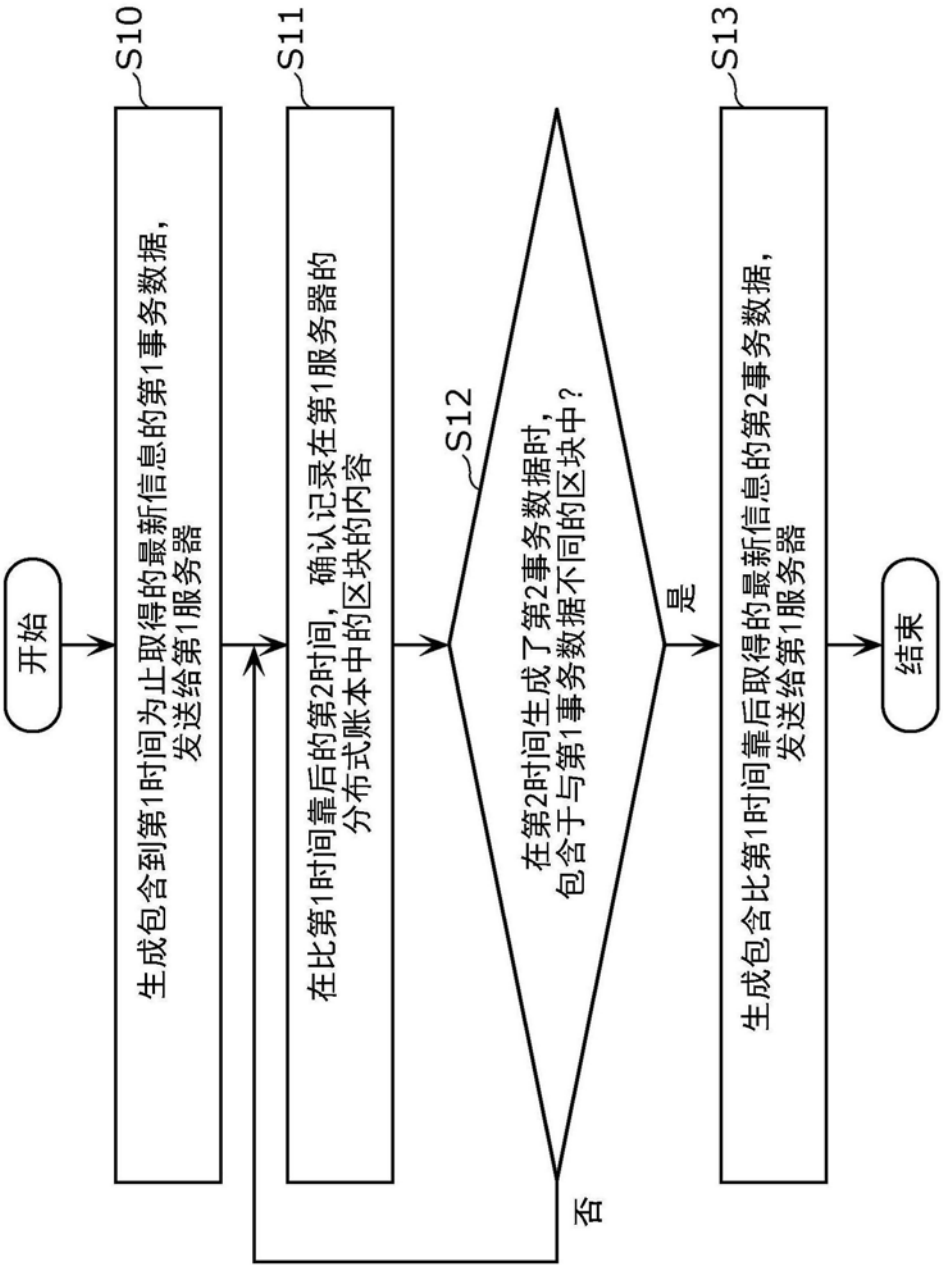

开始
S10
生成包含到第1时间为止取得的最新信息的第1事务数据，
发送给第1服务器
S11
在比第1时间靠后的第2时间，确认记录在第1服务器的
分布式账本中的区块的内容
S12
在第2时间生成了第2事务数据时，
包含于与第1事务数据不同的区块中？
是
否
S13
生成包含比第1时间靠后取得的最新信息的第2事务数据，
发送给第1服务器
结束

图9

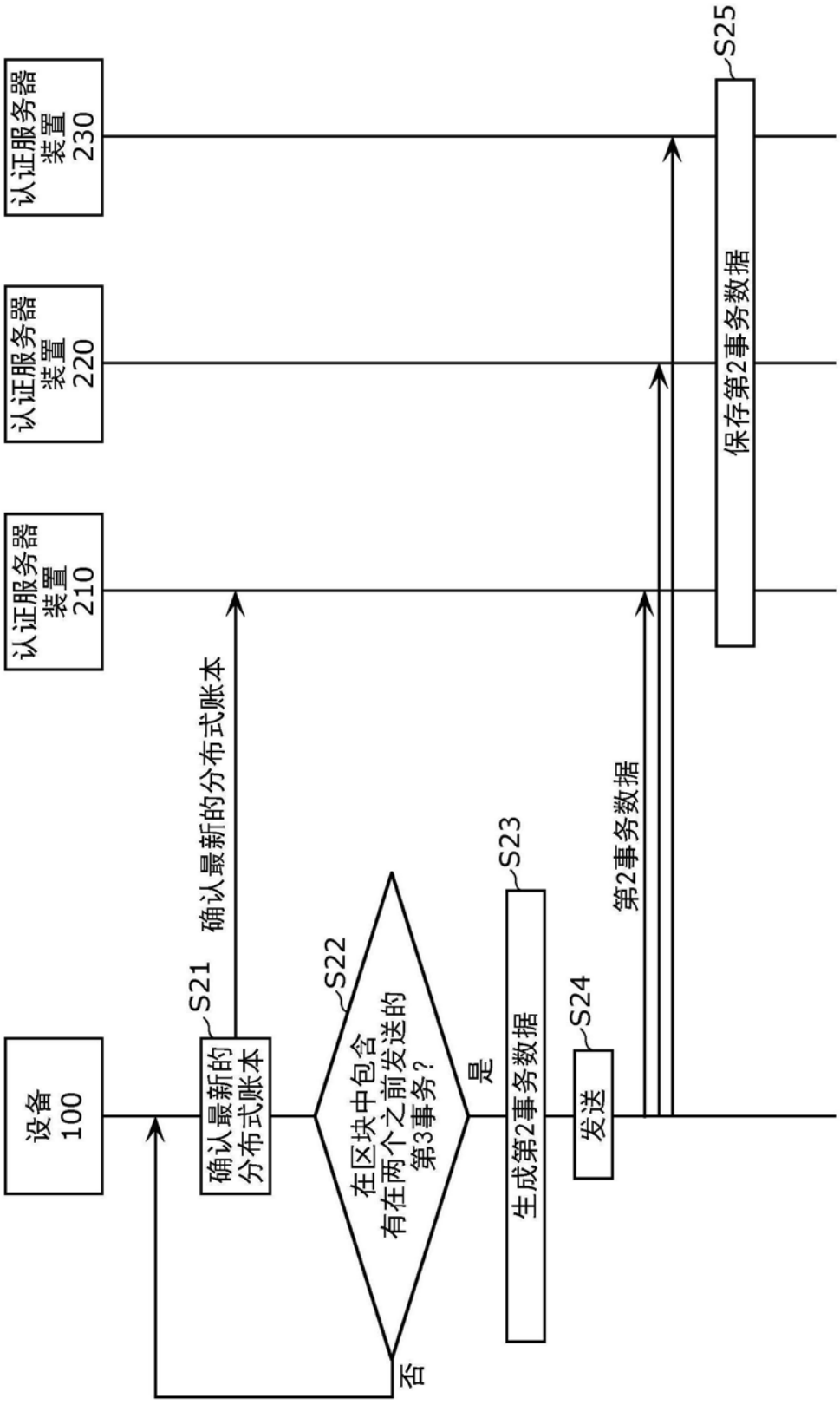

设备
100
确认最新的
分布式账本
S21
确认最新的分布式账本
认证服务器
装置
210
认证服务器
装置
220
认证服务器
装置
230
S22
在区块中包含
有在两个之前发送的
第3事务?
否
是
S23
生成第2事务数据
S24
发送
第2事务数据
S25
保存第2事务数据

图10

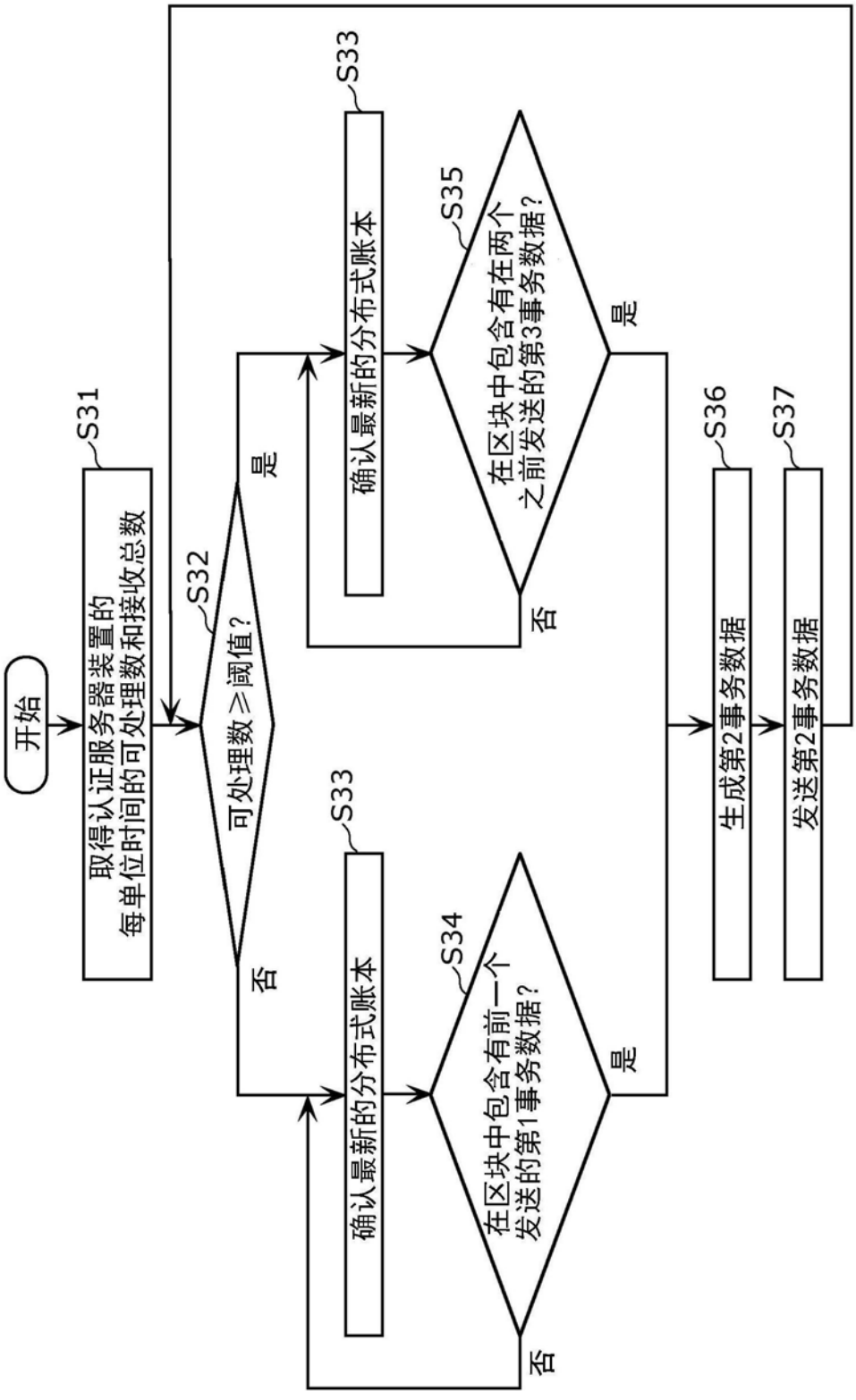

开始
取得认证服务器装置的
每单位时间的可处理数和接收总数
S31
可处理数≥阈值?
S32
是
否
确认最新的分布式账本
S33
在区块中包含有在两个
之前发送的第3事务数据?
S35
是
否
确认最新的分布式账本
S33
在区块中包含有前一个
发送的第1事务数据?
S34
是
否
生成第2事务数据
S36
发送第2事务数据
S37

图11

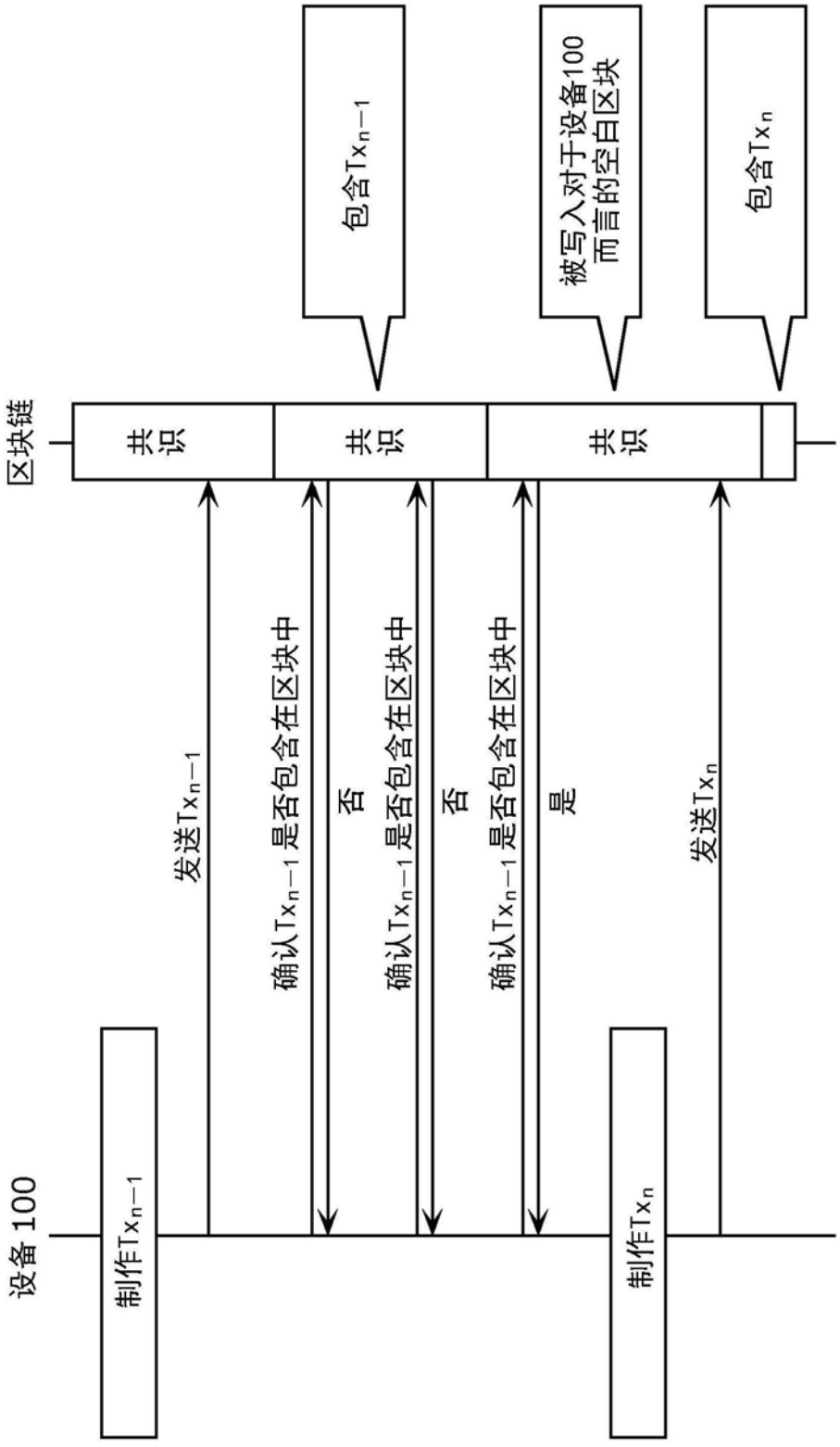

区块链
共识
共识
共识
包含Tx$_{n-1}$
被写入对于设备100而言的空白区块
包含Tx$_n$
设备 100
制作Tx$_{n-1}$
制作Tx$_n$
发送Tx$_{n-1}$
确认Tx$_{n-1}$是否包含在区块中
否
确认Tx$_{n-1}$是否包含在区块中
否
确认Tx$_{n-1}$是否包含在区块中
是
发送Tx$_n$

图12

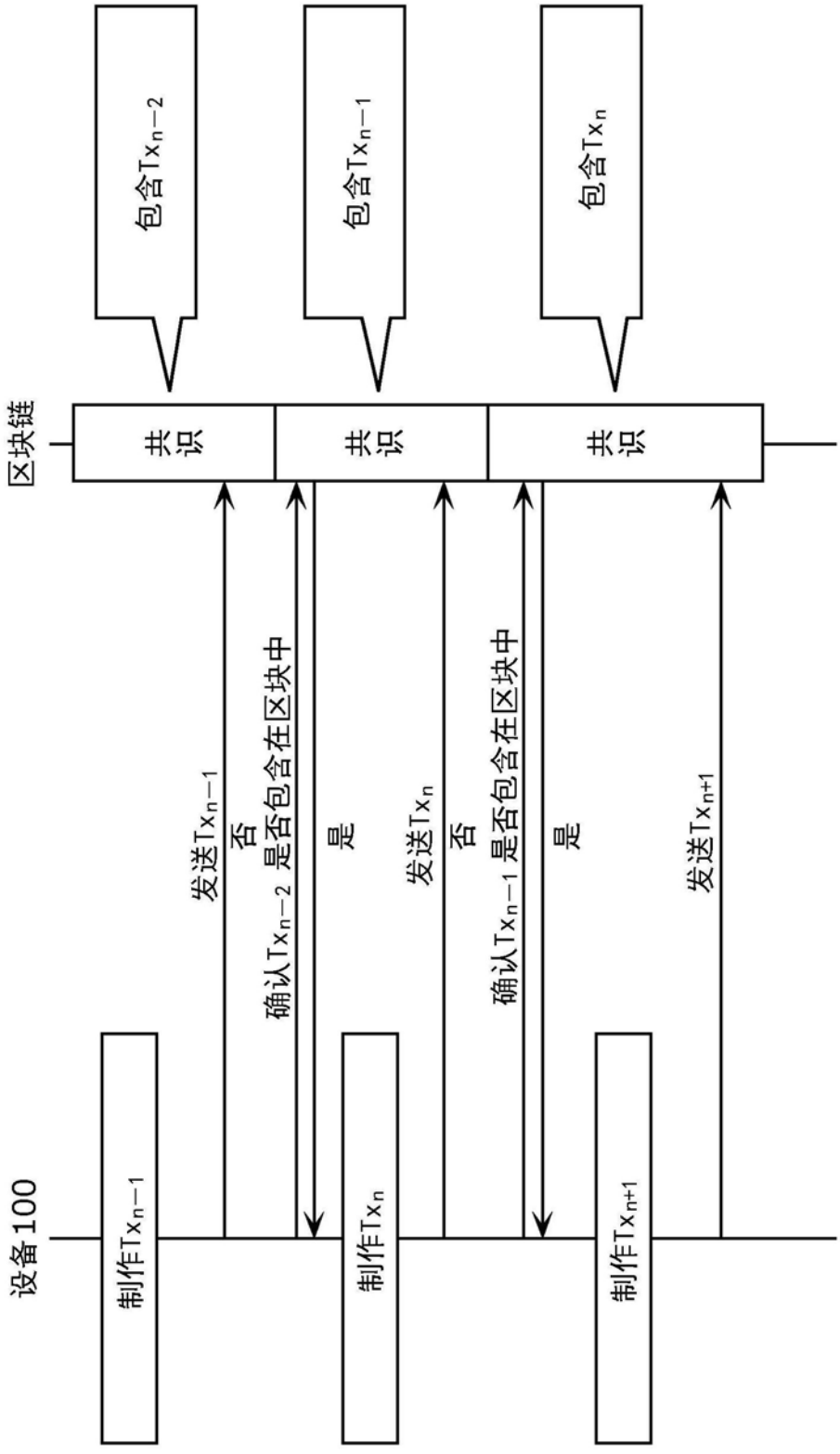

包含Tx$_{n-2}$
包含Tx$_{n-1}$
包含Tx$_n$
区块链
共识
共识
共识
发送Tx$_{n-1}$
否
确认Tx$_{n-2}$是否包含在区块中
是
发送Tx$_n$
否
确认Tx$_{n-1}$是否包含在区块中
是
发送Tx$_{n+1}$
设备100
制作Tx$_{n-1}$
制作Tx$_n$
制作Tx$_{n+1}$

图13

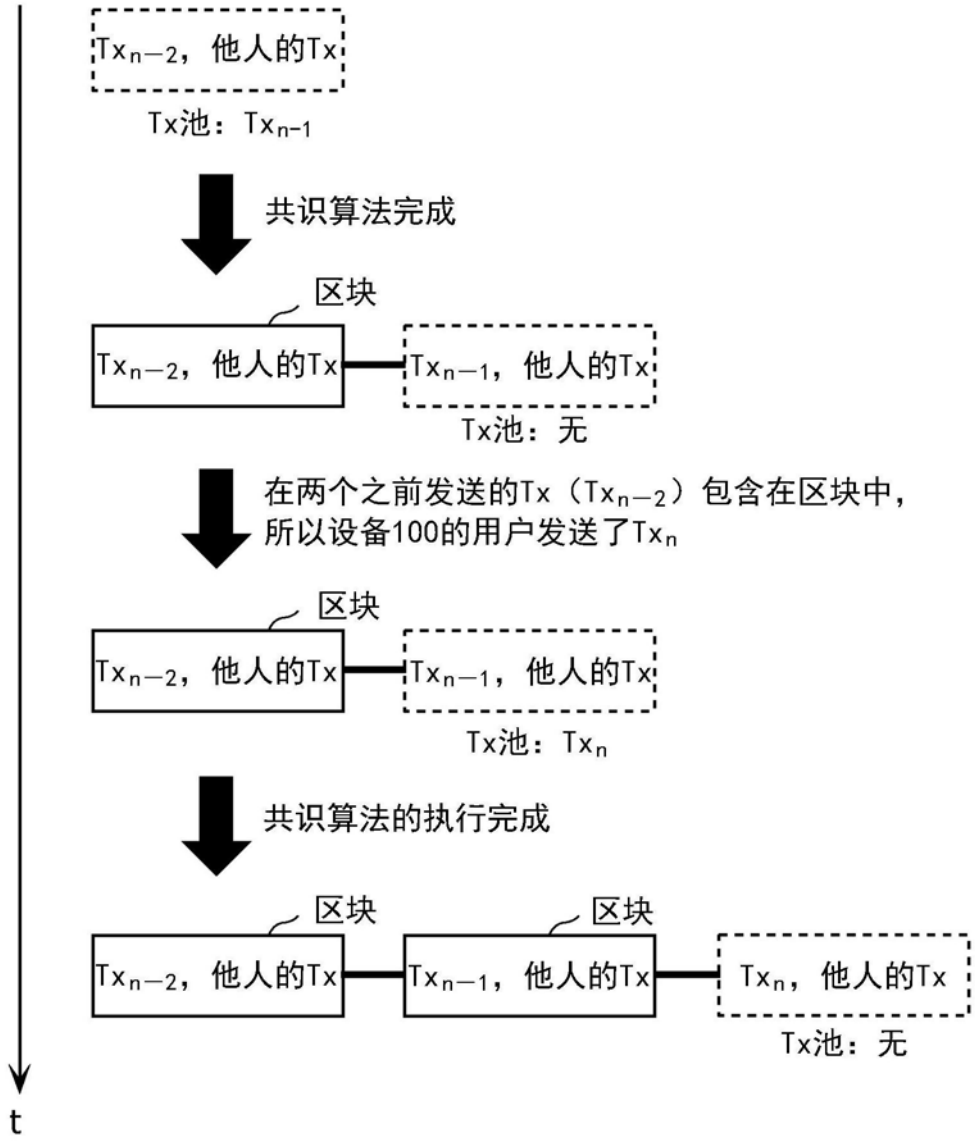

Tx_{n-2}，他人的Tx
Tx池：Tx_{n-1}
共识算法完成
区块
Tx_{n-2}，他人的Tx
Tx_{n-1}，他人的Tx
Tx池：无
在两个之前发送的Tx（Tx_{n-2}）包含在区块中，
所以设备100的用户发送了Tx_n
区块
Tx_{n-2}，他人的Tx
Tx_{n-1}，他人的Tx
Tx池：Tx_n
共识算法的执行完成
区块
区块
Tx_{n-2}，他人的Tx
Tx_{n-1}，他人的Tx
Tx_n，他人的Tx
Tx池：无
t

图14