(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 115004630 A
(43)申请公布日 2022.09.02

(21)申请号 202180011120.X
(22)申请日 2021.01.21
(30)优先权数据
62/968,425 2020.01.31 US
(85)PCT国际申请进入国家阶段日
2022.07.25
(86)PCT国际申请的申请数据
PCT/JP2021/002084 2021.01.21
(87)PCT国际申请的公布数据
WO2021/153421 JA 2021.08.05
(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
(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.
H04L 9/32(2006.01)
H04L 9/08(2006.01)

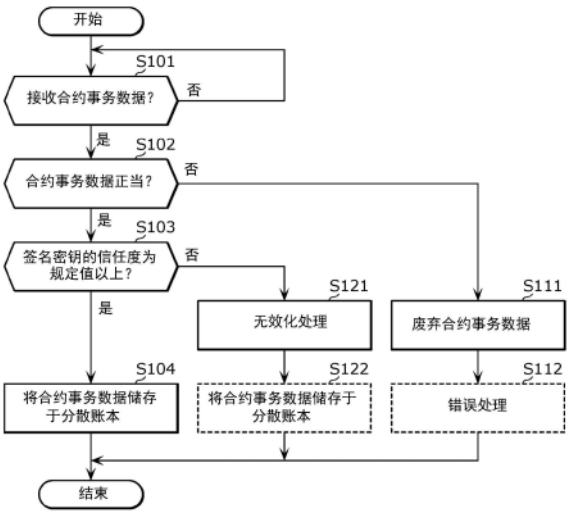
权利要求书3页 说明书16页 附图11页

(54)发明名称

控制方法、服务器以及程序

(57)摘要

在具备保有分散账本的多个服务器的信息管理系统中,该多个服务器中的一个服务器所执行的控制方法,接收包含使用各自与信任度相关联的多个签名密钥中的某签名密钥而制作的签名的事务数据,所述多个签名密钥用户所保有的多个签名密钥(S101),进行与接收到的事务数据中包含的签名相关联的信任度是否为规定值以上的判定(S103),在判定中判定为信任度为规定值以上的情况下,将事务数据储存于分散账本(S104),在判定中判定为信任度小于规定值的情况下,执行使事务数据无效的无效化处理(S121)。



CN 115004630 A

1.一种控制方法,是在具备保有分散账本的多个服务器的信息管理系统中,该多个服务器中的一个服务器所执行的控制方法,在所述控制方法中,

接收包含使用各自与信任度相关联的多个签名密钥中的某签名密钥而制作的签名的事务数据,所述多个签名密钥是用户所保有的多个签名密钥,

进行与接收到的所述事务数据中包含的所述签名的制作所使用的所述签名密钥相关联的所述信任度是否为规定值以上的判定,

在所述判定中判定为所述信任度为所述规定值以上的情况下,将所述事务数据储存于所述分散账本,

在所述判定中判定为所述信任度小于所述规定值的情况下,执行将所述事务数据无效的无效化处理。

2.根据权利要求1所述的控制方法,

所述规定值是向所述用户要求签名的赋予的用户即要求用户所确定的、所述签名的制作所使用的所述签名密钥被要求的信任度即要求信任度,

所述事务数据还包含所述要求信任度。

3.根据权利要求1所述的控制方法,

所述规定值是根据所述事务数据的内容而预先确定的信任度。

4.根据权利要求1至3中任一项所述的控制方法,

所述无效化处理包含对所述事务数据赋予表示所述事务数据无效的无效信息,并将被赋予了所述无效信息的所述事务数据储存于所述分散账本的处理。

5.根据权利要求1至3中任一项所述的控制方法,

所述无效化处理包含不将所述事务数据储存于所述分散账本而废弃的处理。

6.根据权利要求1至5中任一项所述的控制方法,

在接收到所述事务数据的情况下,

通过接收到的所述事务数据中包含的所述签名,执行所述事务数据的验证处理,在所述验证处理中验证成功时,进行所述判定。

7.根据权利要求2所述的控制方法,

所述事务数据还包含所述要求用户的签名,

在接收到所述事务数据的情况下,

通过接收到的所述事务数据中包含的所述要求用户的签名以及所述用户的签名中的各个签名,执行所述事务数据的验证处理,在所述验证处理中验证成功了的情况下,进行所述判定。

8.一种控制方法,是在具备保有分散账本的多个服务器的认证系统中,该多个服务器中的一个服务器所执行的控制方法,在所述控制方法中,

接收包含使用与一个以上的属性相关联的签名密钥而制作的签名的事务数据,所述签名密钥是用户所保有的签名密钥,

进行与接收到的所述事务数据中包含的所述签名的制作所使用的所述签名密钥相关联的所述一个以上的属性是否包含规定的一个以上的规定属性中的至少一个规定属性的判定,

在所述判定中,在判定为所述一个以上的属性包含所述至少一个规定属性的情况下,

将所述事务数据储存于所述分散账本，

在所述判定中，在判定为所述一个以上的属性不包含所述至少一个规定属性的情况下，执行使所述事务数据无效的无效化处理。

9.根据权利要求8所述的控制方法，

在所述判定中，

进行与接收到的所述事务数据中包含的所述签名的制作所使用的所述签名密钥相关联的所述一个以上的属性是否包含全部的所述规定的一个以上的规定属性的判定，

在判定为所述一个以上的属性包含全部的所述规定的一个以上的规定属性的情况下，将所述事务数据储存于所述分散账本，

在判定为所述一个以上的属性不包含全部的所述规定的一个以上的规定属性的情况下，执行使所述事务数据无效的无效化处理。

10.根据权利要求8或9所述的控制方法，

所述规定属性是向所述用户要求签名的赋予的用户即要求用户所确定的、所述签名被要求的属性即要求属性，

所述事务数据还包含所述要求属性。

11.根据权利要求8至10中任一项所述的控制方法，

所述规定属性是根据所述事务数据的内容而预先确定的属性。

12.根据权利要求8至11中任一项所述的控制方法，

所述无效化处理包含向所述事务数据赋予表示所述事务数据无效的无效信息，并将被赋予了所述无效信息的所述事务数据储存于所述分散账本的处理。

13.根据权利要求8至12中任一项所述的控制方法，

所述无效化处理包含不将所述事务数据储存于所述分散账本而废弃的处理。

14.根据权利要求8至13中任一项所述的控制方法，

在接收到所述事务数据的情况下，

通过接收到的所述事务数据中包含的所述签名，执行所述事务数据的验证处理，在所述验证处理中验证成功时，进行所述判定。

15.根据权利要求10所述的控制方法，

所述事务数据还包含所述要求用户的签名，

在接收到所述事务数据的情况下，

通过接收到的所述事务数据中包含的所述要求用户的签名以及所述用户的签名中的各个签名，执行所述事务数据的验证处理，在所述验证处理中验证成功了的情况下，进行所述判定。

16.一种服务器，是具备保有分散账本的多个服务器的认证系统中的，该多个服务器中的一个服务器，所述服务器具备：

储存有所述分散账本的账本储存部；以及

信任性验证部，

所述信任性验证部接收包含使用各自与信任度相关联的多个签名密钥中的某签名密钥而制作的签名的事务数据，所述多个签名密钥是用户所保有的多个签名密钥，

进行与接收到的所述事务数据中包含的所述签名的制作所使用的所述签名密钥相关

联的所述信任度是否为规定值以上的判定，

在所述判定中判定为所述信任度为所述规定值以上的情况下，将所述事务数据储存于所述分散账本，

在所述判定中判定为所述信任度小于所述规定值的情况下，执行使所述事务数据无效的无效化处理。

17.一种服务器，是在具备保有分散账本的多个服务器的信息管理系统中，该多个服务器中的一个服务器，所述服务器具备：

储存有所述分散账本的账本储存部；以及

属性验证部，

所述属性验证部接收包含使用与一个以上的属性相关联的签名密钥而制作的签名的事务数据，所述签名密钥是用户所保有的签名密钥，

进行与接收到的所述事务数据中包含的所述签名的制作所使用的所述签名密钥相关联的所述一个以上的属性是否包含规定的一个以上的规定属性中的至少一个规定属性的判定，

在所述判定中，在判定为所述一个以上的属性包含所述至少一个规定属性的情况下，将所述事务数据储存于所述分散账本，

在所述判定中，在判定为所述一个以上的属性不包含所述至少一个规定属性的情况下，执行使所述事务数据无效的无效化处理。

18.一种程序，

使计算机执行权利要求1至15中任一项所述的控制方法。

控制方法、服务器以及程序

技术领域

[0001] 本发明涉及控制方法、服务器以及程序。

背景技术

[0002] 具有通过分散账本来管理信息的技术。分散账本中储存有包含被管理的信息、以及关于该信息而被制作的电子签名(也仅称为签名)的事务数据。

[0003] 现有技术文献

[0004] 专利文献

[0005] 专利文献1:日本特开第2019－184908号公报

发明内容

[0006] 发明要解决的课题

[0007] 本发明提供具有更高的信任性而在分散账本中管理信息的控制方法等。

[0008] 用于解决课题的手段

[0009] 本发明的一形态的控制方法,是在具备保有分散账本的多个服务器的信息管理系统中,该多个服务器中的一个服务器所执行的控制方法,在所述控制方法中,接收包含使用各自与信任度相关联的多个签名密钥中的某签名密钥而制作的签名的事务数据,所述多个签名密钥是用户所保有的多个签名密钥,进行与接收到的所述事务数据中包含的所述签名的制作所使用的所述签名密钥相关联的所述信任度是否为规定值以上的判定,在所述判定中判定为所述信任度为所述规定值以上的情况下,将所述事务数据储存于所述分散账本,在所述判定中判定为所述信任度小于所述规定值的情况下,执行使所述事务数据无效的无效化处理。

[0010] 另外,这些总括性或具体形态,也可以由系统、装置、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、装置、集成电路、计算机程序以及记录介质的任意组合实现。

[0011] 发明效果

[0012] 本发明的控制方法能够具有更高的信任性而在分散账本中管理信息。

附图说明

[0013] 图1是示意地示出实施方式1中的信息管理系统的构成的方框图。

[0014] 图2是示出实施方式1中的终端的功能结构的第一例的方框图。

[0015] 图3是示出实施方式1中的终端的功能结构的第二例的方框图。

[0016] 图4是示出实施方式1中的认证服务器的功能结构的一个例子的方框图。

[0017] 图5是示出实施方式1中的合约数据的一个例子的说明图。

[0018] 图6是示出实施方式1中的合约事务数据的一个例子的说明图。

[0019] 图7是示出实施方式1中的认证服务器的处理的流程图。

[0020] 图8是示出实施方式1中的信息管理系统的处理的时序图。

[0021] 图9是示出实施方式1的变形例中的信息管理系统的处理的时序图。

[0022] 图10是示出实施方式2中的认证服务器的功能结构的一个例子的方框图。

[0023] 图11是示出实施方式2中的合约数据的一个例子的说明图。

[0024] 图12是示出实施方式2中的合约事务数据的一个例子的说明图。

[0025] 图13是示出实施方式2中的认证服务器的处理的流程图。

[0026] 图14是示出区块链的数据构造的说明图。

[0027] 图15是示出事务数据的数据构造的说明图。

具体实施方式

[0028] (作为本发明的基础的知识)

[0029] 本发明人发现关于“背景技术”栏中记载的与信息的管理相关的技术会产生以下问题。

[0030] 存在通过分散账本来管理信息的技术。在分散账本中储存有包含被管理的信息、以及关于该信息而被制作的电子签名(也仅称作签名)的事务数据,并以实质上不能篡改的方式被管理。

[0031] 签名通过对于被管理的信息进行使用了用户的签名密钥的运算而生成。用户的签名密钥能够由各用户自由地制作,此外,如果存在用户间的合意则能够自由地进行签名密钥的交换。因此,能够保有其他的用户的签名密钥,并制作伪装成该用户而对事务数据赋予的签名。

[0032] 因此,被赋予给通过分散账本管理的信息的签名,具有赋予了该签名的签名者是否确实是该签名者这一点的信任性不高的问题。

[0033] 本发明提供具有更高的信任性在分散账本中管理信息的控制方法等。

[0034] 本发明控制方法,是在具备保有分散账本的多个服务器的信息管理系统中,该多个服务器中的一个服务器所执行的控制方法,在所述控制方法中,接收包含使用各自与信任度相关联的多个签名密钥中的某签名密钥而制作的签名的事务数据,所述多个签名密钥是用户所保有的多个签名密钥,进行与接收到的所述事务数据中包含的所述签名的制作所使用的所述签名密钥相关联的所述信任度是否为规定值以上的判定,在所述判定中判定为所述信任度为所述规定值以上的情况下,将所述事务数据储存于所述分散账本,在所述判定中判定为所述信任度小于所述规定值的情况下,执行使所述事务数据无效的无效化处理。

[0035] 根据上述形态,基于事务数据中包含的签名的制作所使用的签名密钥的信任度,推断与赋予了该签名的用户相关的信任性,使用该信任性控制是将该事务数据储存于分散账本,还是设为无效。并且,在签名密钥的信任度为规定值以上的情况下,将事务数据储存于分散账本,另一方面,在相反的情况下,使事务数据无效化,因此,能够将信任度比较高的事务数据储存于分散账本。如此,根据上述控制方法,能够具有更高的信任性而在分散账本中管理信息。

[0036] 此外,也可以是,所述规定值是向所述用户要求签名的赋予的用户即要求用户所确定的、所述签名的制作所使用的所述签名密钥被要求的信任度即要求信任度,所述事务

数据还包含所述要求信任度。

[0037] 根据上述形态，将要求用户所确定的要求信任度用作规定值，能够将信任度比较高的事务数据储存于分散账本。由此，根据上述控制方法，能够更加容易地具有更高的信任性而在分散账本中管理信息。

[0038] 此外，也可以是，所述规定值是根据所述事务数据的内容而预先确定的信任度。

[0039] 根据上述形态，将根据事务数据的内容而预先确定的信任度用作规定值，能够将信任度比较高的事务数据储存于分散账本。由此，根据上述控制方法，能够更加容易地具有更高的信任性而在分散账本中管理信息。

[0040] 此外，也可以是，所述无效化处理包含对所述事务数据赋予表示所述事务数据无效的无效信息，并将被赋予了所述无效信息的所述事务数据储存于所述分散账本的处理。

[0041] 根据上述形态，将签名的制作所使用的签名密钥的信任度小于规定值的事务数据赋予无效信息并储存于分散账本，并且，将信任度比较高的事务数据作为有效的事务数据储存于分散账本。如此，能够在签名密钥的信任度为规定值以上时以及小于规定值时均将事务数据储存于分散账本并进行管理。由此，根据上述控制方法，能够具有更高的信任性而在分散账本中管理全部的事务数据。

[0042] 此外，也可以是，所述无效化处理包含不将所述事务数据储存于所述分散账本而废弃的处理。

[0043] 根据上述形态，废弃签名的制作所使用的签名密钥的信任度小于规定值的事务数据，并且，将信任度比较高的事务数据作为有效的事务数据储存于分散账本。如此，不将签名密钥的信任度小于规定值的事务数据储存于分散账本，因此，能够抑制储存分散账本的存储装置的存储容量的增大。由此，根据上述控制方法，能够具有更高的信任性并在抑制必要的存储装置的存储容量的基础上在分散账本中管理信息。

[0044] 此外，也可以是，在接收到所述事务数据的情况下，通过接收到的所述事务数据中包含的所述签名，执行所述事务数据的验证处理，在所述验证处理中验证成功时，进行所述判定。

[0045] 根据上述形态，通过对于签名的验证成功了的事务数据进行关于签名的制作所使用签名密钥的信任度的判定，确认了事务数据没有被篡改或者破坏。由此，根据上述控制方法，能够在具有更高的信任性并且没有篡改等的状态下，在分散账本中管理信息。

[0046] 此外，也可以是，所述事务数据还包含所述要求用户的签名，在接收到所述事务数据的情况下，通过接收到的所述事务数据中包含的所述要求用户的签名以及所述用户的签名中的各个签名，执行所述事务数据的验证处理，在所述验证处理中验证成功了的情况下，进行所述判定。

[0047] 根据上述形态，通过对于多个签名的验证成功了的事务数据进行关于签名的制作所使用的签名密钥的信任度的判定，能够确认事务数据没有被篡改或者破坏、以及由多方完成了事务数据的内容的确认。由此，根据上述控制方法，能够在可以进行基于多个用户的内容的确认的基础上，具有更高的信任性而在分散账本中管理信息。

[0048] 此外，本发明的一形态的控制方法，是在具备保有分散账本的多个服务器的认证系统中，该多个服务器中的一个服务器所执行的控制方法，在所述控制方法中，接收包含使用与一个以上的属性相关联的签名密钥而制作的签名的事务数据，所述签名密钥是用户所

保有的签名密钥，进行与接收到的所述事务数据中包含的所述签名的制作所使用的所述签名密钥相关联的所述一个以上的属性是否包含规定的一个以上的规定属性中的至少一个规定属性的判定，在所述判定中，在判定为所述一个以上的属性包含所述至少一个规定属性的情况下，将所述事务数据储存于所述分散账本，在所述判定中，在判定为所述一个以上的属性不包含所述至少一个规定属性的情况下，执行使所述事务数据无效的无效化处理。

[0049] 根据上述形态，基于事务数据中包含的签名的制作所使用的签名密钥的属性推断与赋予了该签名的用户相关的信任性，使用该信任性控制是将该事务数据储存于分散账本，还是设为无效。并且，在签名密钥的属性包含规定属性的至少一个的情况下将事务数据储存于分散账本，另一方面，在相反的情况下使事务数据无效化，因此，能够将信任度比较高的事务数据储存于分散账本。如此，根据上述控制方法，能够具有更高的信任性在分散账本中管理信息。

[0050] 此外，也可以是，在所述判定中，进行与接收到的所述事务数据中包含的所述签名的制作所使用的所述签名密钥相关联的所述一个以上的属性是否包含全部的所述规定的一个以上的规定属性的判定，在判定为所述一个以上的属性包含全部的所述规定的一个以上的规定属性的情况下，将所述事务数据储存于所述分散账本，在判定为所述一个以上的属性不包含全部的所述规定的一个以上的规定属性的情况下，执行使所述事务数据无效的无效化处理。

[0051] 根据上述形态，在签名密钥的属性包含全部的规定属性的情况下，将事务数据储存于分散账本，另一方面，在相反的情况下使事务数据无效化，因此，能够将信任度比较高的事务数据储存于分散账本。如此，根据上述控制方法，能够具有更高的信任性在分散账本中管理信息。

[0052] 此外，也可以是，所述规定属性是向所述用户要求签名的赋予的用户即要求用户所确定的、所述签名所要求的属性即要求属性，所述事务数据还包含所述要求属性。

[0053] 根据上述形态，将要求用户所确定的要求属性用作规定属性，能够将信任度比较高的事务数据储存于分散账本。由此，根据上述控制方法，能够更加容易地具有更高的信任性在分散账本中管理信息。

[0054] 此外，也可以是，所述规定属性是根据所述事务数据的内容而预先确定的属性。

[0055] 根据上述形态，将根据事务数据的内容而预先确定的属性用作规定属性，能够将信任度比较高的事务数据储存于分散账本。由此，根据上述控制方法，能够更加容易地具有更高的信任性而在分散账本中管理信息。

[0056] 此外，也可以是，所述无效化处理包含向所述事务数据赋予表示所述事务数据无效的无效信息，并将被赋予了所述无效信息的所述事务数据储存于所述分散账本的处理。

[0057] 根据上述形态，将签名的制作所使用的签名密钥的属性不包含规定属性中的至少一个的事务数据赋予无效信息而储存于分散账本，并且，将签名的属性包含规定属性中的至少一个的事务数据作为有效的事务数据而储存于分散账本。如此，在签名密钥的属性包含规定属性中的至少一个时以及不包含规定属性中的至少一个时均能够将事务数据储存于分散账本并进行管理。由此，根据上述控制方法，能够具有更高的信任性而在分散账本管理全部的事务数据。

[0058] 此外，也可以是，所述无效化处理包含不将所述事务数据储存于所述分散账本而

废弃的处理。

[0059] 根据上述形态，废弃签名的制作所使用的签名密钥的属性不包含规定属性中的至少一个的事务数据，并且，将签名的属性包含规定属性中的至少一个的事务数据作为有效的事务数据储存于分散账本。如此，不将签名密钥的属性不包含规定属性中的至少一个的事务数据储存于分散账本，因此，能够抑制储存分散账本的存储装置的存储容量的增大。由此，根据上述控制方法，能够具有更高的信任性，并在抑制必要的存储装置的存储容量的基础上，在分散账本中管理信息。

[0060] 此外，也可以是，在接收到所述事务数据的情况下，通过接收到的所述事务数据中包含的所述签名，执行所述事务数据的验证处理，在所述验证处理中验证成功时，进行所述判定。

[0061] 根据上述形态，通过对于签名的验证成功了的事务数据进行关于签名的制作所使用的签名密钥的属性的判定，确认了事务数据没有被篡改或者破坏。由此，根据上述控制方法，能够在具有更高的信任性，并且没有篡改等的状态下，在分散账本中管理信息。

[0062] 此外，所述事务数据还包含所述要求用户的签名，在接收到所述事务数据的情况下，分别通过接收到的所述事务数据中包含的所述要求用户的签名以及所述用户的签名，执行所述事务数据的验证处理，在所述验证处理中验证成功了的情况下，进行所述判定。

[0063] 根据上述形态，对于多个签名的验证成功了的事务数据进行关于签名的制作所使用的签名密钥的属性的判定，能够确认事务数据没有被篡改或者破坏、以及由多方完成了事务数据的内容的确认。由此，根据上述控制方法，能够在可以进行基于多个用户的内容的确认的基础上，具有更高的信任性而在分散账本中管理信息。

[0064] 此外，本发明的一形态的服务器，是在具备保有分散账本的多个服务器的认证系统中的，该多个服务器中的一个服务器，所述服务器具备：储存有所述分散账本的账本储存部；以及信任性验证部，所述信任性验证部接收包含使用各自与信任度相关联的多个签名密钥中的某签名密钥而制作的签名的事务数据，所述多个签名密钥是用户所保有的多个签名密钥，进行与接收到的所述事务数据中包含的所述签名的制作所使用的所述签名密钥相关联的所述信任度是否为规定值以上的判定，在所述判定中判定为所述信任度为所述规定值以上的情况下，将所述事务数据储存于所述分散账本，在所述判定中判定为所述信任度小于所述规定值的情况下，执行使所述事务数据无效的无效化处理。

[0065] 根据上述形态，能够实现与上述控制方法相同的效果。

[0066] 此外，本发明的一形态的种服务器，是在具备保有分散账本的多个服务器的信息管理系统中，该多个服务器中的一个服务器，所述服务器具备：储存有所述分散账本的账本储存部；以及属性验证部，所述属性验证部接收包含使用与一个以上的属性相关联的签名密钥而制作的签名的事务数据，所述签名密钥是用户所保有的签名密钥，进行与接收到的所述事务数据中包含的所述签名的制作所使用的所述签名密钥相关联的所述一个以上的属性是否包含规定的一个以上的规定属性中的至少一个规定属性的判定，在所述判定中，在判定为所述一个以上的属性包含所述至少一个规定属性的情况下，将所述事务数据储存于所述分散账本，在所述判定中，在判定为所述一个以上的属性不包含所述至少一个规定属性的情况下，执行使所述事务数据无效的无效化处理。

[0067] 根据上述形态，实现与上述控制方法相同的效果。

[0068] 此外，本发明的一形态的程序是使计算机执行上述控制方法的程序。

[0069] 根据上述形态，实现与上述控制方法相同的效果。

[0070] 另外，这些总括性或具体形态，可以由系统、装置、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、装置、集成电路、计算机程序以及记录介质的任意组合实现。

[0071] 以下，参照附图具体地说明实施方式。

[0072] 另外，以下说明的实施方式，均示出总括性或具体例子。以下的实施方式所示的数值、形状、材料、构成要素、构成要素的配置位置以及连接方式、步骤、步骤的顺序等是一个例子，其主旨并非是限定本发明。并且，对于以下的实施方式的构成要素中的示出最上位概念的实施方案中没有记载的构成要素，作为任意的构成要素而被说明。

[0073] (实施方式1)

[0074] 在本实施方式中，说明具有更高的信任性而在分散账本中管理信息的信息管理系统以及其控制方法等。

[0075] 图1是示意地示出本实施方式中的信息管理系统1的构成的方框图。

[0076] 信息管理系统1是使用分散账本管理各种信息的系统。

[0077] 这里，以信息管理系统1管理的信息是与用户A与用户B之间签订的买卖合约相关的信息的情况为例子进行说明。

[0078] 如图1所示，信息管理系统1具备认证服务器310、320以及330。

[0079] 认证服务器310是使用分散账本管理与买卖合约相关的信息的服务器装置。认证服务器310是保有分散账本的多个服务器中的一个服务器。认证服务器310所保有的分散账本中储存有包含与买卖合约相关的信息的事务数据(也称作合约事务数据)。合约事务数据包含使用与信任度相关联的签名密钥而赋予的签名。之后详细地说明认证服务器310的处理、信任度以及合约事务数据的数据构造等。

[0080] 认证服务器320以及330与认证服务器310同样，是使用分散账本管理与买卖合约相关的信息的服务器装置，与认证服务器310之间独立地动作。

[0081] 认证服务器310、320以及330(也称作认证服务器310等)以能够通信的方式连接即可，其物理位置可以在任何地方。此外，认证服务器310等可以是由单一的企业或者个人所保有或者管理的服务器，也可以是由多个企业或者个人所保有或者管理的服务器。

[0082] 另外，以认证服务器310等的台数为3台的情况为例子进行说明，但也可以是更多的台数。

[0083] 终端100是用户A所保有的信息终端。终端100接受用户A进行的与合约相关的操作，基于该操作进行与认证服务器310等或者终端200之间的通信。此外，终端100从认证服务器310等或者终端200接收与合约相关的信息，通过画面显示或者语音等向用户A提示。终端100，例如是智能手机、平板或者个人计算机等。

[0084] 终端200是用户B所保有的信息终端。终端200接受基于用户B的与合约相关的操作，基于该操作进行与认证服务器310等或者终端100之间的通信。此外，终端200从认证服务器310等或者终端100接收与合约相关的信息，通过画面显示或者语音等向用户B提示。终端200，例如是智能手机、平板或者个人计算机等。

[0085] 另外，终端100与终端200当然也能够不经由认证服务器310等进行通信。

[0086] 另外，信息管理系统1也可以还具备用户A所保有的终端100以及用户B所保有的终端200中的一方或者双方。

[0087] 以下，作为一个例子，说明信息管理系统1使用分散账本管理与用户A及用户B之间的买卖合约相关的信息的情况下的信息管理系统1、终端100以及200的处理。这里，设为用户A是要以不确定的人为对象销售商品的销售者，用户B是要购买用户A所销售的商品的购买者。信息管理系统1管理与用户A根据用户B的购买的要求向用户B销售商品的情况下的买卖合约相关的信息。

[0088] 图2是示出本实施方式中的终端的功能结构的第一例的终端100的功能结构的方框图。

[0089] 如图2所示，终端100具备合约决定部101、条件决定部102、数据制作部103以及通信部104。终端100所具备的各功能部可以通过终端100所具备的CPU(Central Processing Unit，中央处理器)(未图示)使用存储器执行规定的程序而实现。

[0090] 合约决定部101是决定用户A与用户B之间签订的合约的内容(也称作合约内容)，并生成表示合约内容的信息的功能部。具体而言，合约决定部101决定用户A与用户B之间签订的买卖合约的内容。买卖合约的内容中例如可以包含对用户A向用户B销售的商品的信息(商品编号等)、该商品的数量、交付日期、交付目的地以及价格等进行确定的信息。

[0091] 此外，合约决定部101对签订合约的一方(也称作签订者)进行确定。也可以是，在决定合约内容的时刻，不确定全部的签订者。该情况下，合约决定部101生成至少对在决定合约内容的时刻被确定的签订者进行确定的信息即可。

[0092] 条件决定部102是决定与向用户B要求的签名的信任度相关的条件的功能部，用户B是与用户A签订合约的对象。与向签订合约的对象要求的签名的信任度相关的条件的一个例子是签订合约的对象对合约事务数据赋予的签名的信任度为规定值以上这一条件，对这种情况进行说明，但并不限定于此。规定值，例如是用户A即向作为签订合约的对象的用户B要求签名的赋予的用户(也称作要求用户)所确定的该签名被要求的信任度即要求信任度。关于信任度之后详细说明。

[0093] 数据制作部103是制作表示用户A与用户B之间签订的合约的内容的合约数据的功能部。数据制作部103取得合约决定部101所决定的合约内容，制作包含合约内容的合约数据。另外，在条件决定部102决定了要求信任度作为规定值的情况下，合约决定部101取得该要求信任度，制作包含上述的合约内容与要求信任度的合约数据。数据制作部103经由通信部104向终端200发送制作的合约数据。

[0094] 另外，在对数据制作部103所制作的合约数据赋予用户A的签名的情况下，数据制作部103通过对表示合约内容的信息进行使用了用户A的签名密钥的运算来制作签名，生成赋予了制作的签名的合约数据。在这种情况下，设为数据制作部103预先保有用户A的签名密钥。

[0095] 通信部104是以能够通信的方式连接于认证服务器310等以及终端200的通信接口。通信部104用于合约数据的发送等。

[0096] 图3是示出作为本实施方式中的终端的功能结构的第二例的终端200的功能结构的方框图。

[0097] 如图3所示，终端200具备密钥储存部201、合约取得部202、签名制作部203、事务制

作部204、以及通信部205。终端200所具备的各功能部通过终端200所具备的CPU(未图示)使用存储器执行规定的程序而实现,此外,可以通过存储装置实现。

[0098] 密钥储存部201具有储存有用户B的签名密钥的存储装置。密钥储存部201中储存有用户B的多个签名密钥。用户B的多个签名密钥各自与信任度相关联。这里,信任度是指表示签名密钥的信任的高度的指标。信任度例如是以三个阶段表示签名密钥的信任的高度的指标。这里,三个阶段的信任度表现为意味着比较高的信任度的“金”,意味着中等程度的信任度的“银”以及意味着比较的低的信任度的“铜”。此外,将具有金的信任度的签名密钥以及由该签名密钥生成的签名分别称作“金密钥”以及“金签名”。将具有银的信任度的签名密钥以及由该签名密钥生成的签名分别称作“银密钥”以及“银签名”。将具有铜的信任度的签名密钥以及由该签名密钥生成的签名分别称作“铜密钥”以及“铜签名”。

[0099] 另外,三个阶段的信任度的表现并不局限于此,也可以表现为“高”、“中”以及“低”、或者表现为“3”、“2”以及“1”。此外,信任度的阶段的数量只要是2以上就可以是任意的数量。

[0100] 另外,与签名密钥相关联的信任度可以由各种重要因素决定。例如,与签名密钥相关联的信任度可以由制作该签名密钥的一方决定。例如,也可以是用户自身制作的签名密钥、信任的组织制作的签名密钥、国家、都道府县或市镇村认定的组织制作的签名密钥、上市企业制作的签名密钥、或者被公众认可的企业制作的签名密钥分别与不同的信任度相关联。

[0101] 此外,例如,与签名密钥相关联的信任度也可以根据用户自身被信任的程度而决定。例如,也可以是与进行了对社会有益的行为(捐赠、筹集资金或者志愿活动等)的用户、收入比较高的用户、或者没有犯罪记录的用户的签名密钥相关联的信任度高于与并非如此的用户的签名密钥相关联的信任度。

[0102] 此外,例如,与签名密钥相关联的信任度也可以根据用户向机构委托签名密钥的制作时提出的身份确认文件的不同而决定。例如,也可以根据提出了户籍、居民票、驾驶证、个人编号卡、身份证明书(ID)、面部照片、保险证或者护照中的哪一个而决定信任度。

[0103] 另外,对签名密钥的制作者进行确定的信息也可以以实质上无法篡改的方式通过分散账本来管理。

[0104] 合约取得部202是取得表示合约内容的信息的功能部。合约取得部202取得终端100发送的合约数据所含的合约内容作为表示合约内容的信息。合约取得部202确认取得的合约内容妥当。合约内容的确认可以通过基于计算机的确认处理而实现,也可以通过接受由人进行的合约内容的确认的结果而实现。

[0105] 签名制作部203是制作用户B的签名的功能部。签名制作部203参照事务制作部204所制作的合约事务数据,通过对合约事务数据进行使用了储存于密钥储存部201的用户B的签名密钥的运算来制作签名。签名制作部203向事务制作部204提供制作的签名。

[0106] 事务制作部204是基于合约数据来制作表示合约的内容的合约事务数据的功能部。事务制作部204取得合约取得部202所取得的合约数据,生成包含合约数据所含的信息的合约事务数据。此外,事务制作部204从签名制作部203取得制作的合约事务数据包含的用户B的签名,生成包含取得的签名的合约事务数据。假定事务制作部204从签名制作部203取得的签名是通过具有合约数据所含的要求信任度以上的信任度的签名密钥而制作的签

名。事务制作部204经由通信部205向认证服务器310等发送制作的合约事务数据。

[0107] 通信部205是以能够通信的方式连接于认证服务器310等以及终端100的通信接口。通信部205用于合约数据的接收以及合约事务数据的发送等。

[0108] 图4是示出本实施方式中的认证服务器310的功能结构的一个例子的方框图。

[0109] 如图4所示，认证服务器310具备账本储存部301、信任性验证部302、正当性验证部303、以及通信部304。认证服务器310所具备的各功能部通过认证服务器310所具备的CPU(未图示)使用存储器执行规定的程序而实现，此外，可以通过存储装置实现。

[0110] 账本储存部301具有储存有分散账本的存储装置、以及向分散账本储存合约事务数据的处理部。账本储存部301通过正当性验证部303来验证正当性，此外，取得通过信任性验证部302验证了信任性的合约事务数据，并将其储存于分散账本。此外，账本储存部301将上述合约事务数据向与自身装置不同的认证服务器(即，认证服务器320以及330)发送，使其储存于该认证服务器储存的分散账本中。储存于账本储存部301的分散账本存储有一个以上的合约事务数据，使用哈希值等的特性以篡改困难的方式管理(后述)。

[0111] 另外，分散账本，例如是区块链，以这种情况为例子进行说明，但能够采用其他方式的分散账本(例如，IOTA或者哈希图表等)。另外，分散账本可以在新的事务数据的储存时执行共识算法(例如，PBFT(Practical Byzantine Fault Tolerance，实用拜占庭容错算法)，PoW(Proof of Work，工作量证明)或者PoS(Proof of Stake，权益证明))，也可以不执行。作为不执行共识算法的分散账本技术的一个例子是Hyperledger fabric(超级账本结构)。

[0112] 信任性验证部302是验证合约事务数据的签名的制作所使用的签名密钥的信任性的功能部。信任性验证部302取得由正当性验证部303验证了正当性的合约事务数据(后述)，通过进行被赋予给取得的合约事务数据的签名的制作所使用的签名密钥的信任度是否为规定值以上的判定，来验证合约事务数据的信任性。信任性验证部302在上述判定中判定为签名密钥的信任度为规定值以上的情况下，向账本储存部301提供合约事务数据并使其储存于分散账本。此外，信任性验证部302在上述判定中判定为签名密钥的信任度小于规定值的情况下，执行使合约事务数据无效的无效化处理。无效化处理例如可以包含对合约事务数据赋予表示合约事务数据无效的无效信息，并将被赋予了无效信息的合约事务数据储存于分散账本的处理。此外，无效化处理也可以包含将合约事务数据不储存于分散账本而废弃的处理。另外，也将“签名的制作所使用的签名密钥”称作“签名的签名密钥”。

[0113] 正当性验证部303是验证合约事务数据的正当性的功能部。正当性验证部303经由通信部304接收终端200发送的合约事务数据，使用被赋予给接收到的合约事务数据的签名，验证该合约事务数据所含的信息正当，即没有被篡改或者破坏等。接收到的合约事务数据包含要求信任度。正当性验证部303向信任性验证部302提供验证了正当的、即验证处理成功的合约事务数据。

[0114] 另外，在合约事务数据中包含有合约的签订者即用户A以及B双方的签名的情况下，正当性验证部303分别使用双方的签名进行验证处理。

[0115] 通信部304是以能够通信的方式连接于终端100以及200、及其他认证服务器320以及330的通信接口。通信部304用于合约事务数据的发送或者接收等。

[0116] 以下，说明合约数据以及合约事务数据的例子。

[0117] 图5是示出本实施方式中的合约数据的一个例子的说明图。

[0118] 如图5所示，合约数据包含签订者1以及2、合约内容、要求信任度、及签名1以及2的字段。合约数据由合约决定部101制作。

[0119] 签订者1是表示该合约数据涉及的合约的签订者中的一个合约者的识别信息，只要是能够唯一地对签订者进行确定的识别符就可以是任意的信息。在用户A销售商品的买卖合约中，在合约数据被制作的时刻，决定了签订者中的一方为作为销售者的用户A，因此，签订者1包含用户A的识别信息(图5中记载为“用户A”)。

[0120] 签订者2是表示该合约数据的合约的签订者中的除签订者1之外的一个合约者的识别信息，只要是能够唯一地对签订者进行确定的识别符就可以是任意的信息。在用户A销售商品的买卖合约中，在合约数据被制作的时刻，具有签订者2被确定的情况以及未被确定的情况。在图5中，以签订者2未确定的情况为一个例子示出，包含表示签订者2待定的信息。另外，签订者2例如在用户B被确定的情况下，签订者2包含用户B的识别信息。

[0121] 合约内容是表示买卖合约的内容的信息。合约内容，例如可以包含对销售的商品进行确定的信息(商品编号等)、该商品的数量交付日期、交付目的地以及价格等信息。图5所示的合约内容示出了销售的商品的商品编号为“A001”，该商品的数量为“100”，交付日期为“2020年2月1日”，价格为“10,000日元”。

[0122] 要求信任度是该合约的签名所要求的签名密钥的信任度。要求信任度例如是用户A向用户B要求的签名的制作所使用的签名密钥的信任度。图5所示的要求信任度为金。

[0123] 签名1是该合约数据的合约的签订者中的一个合约者的签名。在用户A销售商品的买卖合约中，在合约数据被制作的时刻，决定了签订者中的一个合约者为用户A，因此，签名1被赋予用户A的金签名。另外，签名1并不是必须的。

[0124] 签名2是该合约数据的合约的签订者中的除签订者1之外的一个合约者的签名。与上述的签订者2中的说明同样，在用户A销售商品的买卖合约中，在合约数据被制作的时刻，具有签订者2已经决定的情况以及未决定的情况。图5中，以签订者2未决定的情况为一个例子示出，示出了尚未赋予签名2这一情况(图5中记载为“—”)。

[0125] 图6是示出本实施方式中的合约事务数据的一个例子的说明图。

[0126] 如图6所示，合约事务数据包含签订者1以及2、合约内容、要求信任度、及签名1以及2。合约事务数据由事务制作部204制作。

[0127] 合约事务数据包含签订者1以及2、合约内容要求信任度、及签名1以及2的字段。合约事务数据所含的各字段的作用与合约数据中相同。但是，在合约事务数据被制作的时刻，决定了签订者中的除用户A以外的一方为用户B，因此，签订者2以及签名2的字段与合约数据不同。

[0128] 在合约事务数据被制作的时刻，用户A以及B双方被确定。在生成合约事务数据的时刻，通过签订者2被确定为用户B，签订者2包含用户B的识别信息(图6中记载为“用户B”)，签名2包含用户B的金签名。

[0129] 图7是示出本实施方式中的认证服务器310的处理的流程图。图7所示的处理示出了认证服务器310在从终端200接收合约事务数据的情况下执行的处理。另外，在认证服务器320或者330从终端200接收合约事务数据的情况下，通过认证服务器320或者330执行相同的处理。

[0130] 在图7中，在步骤S101中，正当性验证部303判定是否接收到合约事务数据。在判定为接收到合约事务数据的情况下(步骤S101中的是)，进入步骤S102，在相反的情况下(步骤S101中的否)，再次执行步骤S101。即，正当性验证部303在步骤S101中待机直到接收合约事务数据。

[0131] 在步骤S102中，正当性验证部303判定在步骤S101中接收到的合约事务数据是否正当。在判定为合约事务数据正当的情况下(步骤S102中的是)，进入步骤S103，在相反的情况下(步骤S102中的否)，进入步骤S111。

[0132] 在步骤S103中，信任性验证部302判定被赋予给在步骤S102中判定为正当的合约事务数据的签名的制作所使用的签名密钥的信任度是否为规定值以上。在判定为签名密钥的信任度为规定值以上的情况下(步骤S103中的是)，进入步骤S104，在相反的情况下(步骤S103中的否)，进入步骤S121。

[0133] 在步骤S104中，账本储存部301将在步骤S103中判定为签名密钥的信任度为规定值以上的合约事务数据储存于分散账本。此外，使上述合约事务数据储存于其他认证服务器的分散账本。在将合约事务数据储存于分散账本时，可以执行共识算法，也可以不执行。

[0134] 在步骤S111中，信任性验证部302废弃在步骤S102中判定为不正当的合约事务数据。

[0135] 在步骤S112中，信任性验证部302与在步骤S111中废弃了合约事务数据这一情况相关联地进行错误处理。错误处理，例如包含将表示废弃了合约事务数据这一情况的信息追加到认证服务器310的日志的处理。另外，也可以不执行步骤S112。

[0136] 在步骤S121中，信任性验证部302对在步骤S103中判定为不正当的合约事务数据执行无效化处理。

[0137] 在步骤S122中，在步骤S121的无效化处理中合约事务数据被赋予了无效信息的情况下，账本储存部301将被赋予了无效信息的合约事务数据储存于分散账本。关于共识算法的执行，与步骤S104中的情况相同。

[0138] 图8是示出本实施方式中的信息管理系统1的处理的时序图。图8所示的处理示出了认证服务器310在从终端200接收合约事务数据的情况下执行的处理。另外，认证服务器320或者330在从终端200接收合约事务数据的情况下也执行相同的处理。另外，关于认证服务器310的处理中与图7所记载的相同的内容，有时标注相同的附图标记省略详细的说明。

[0139] 在步骤S201中，终端100的数据制作部103制作合约数据。制作的合约数据中包含要求信任度。

[0140] 在步骤S202中，终端100的数据制作部103向终端200发送在步骤S201中制作的合约数据。终端200的合约取得部202接收被发送的合约数据。

[0141] 在步骤S203中，终端200的合约取得部202确认在步骤S202中接收的合约数据所含的合约内容妥当。

[0142] 在步骤S204中，终端200的签名制作部203使用用户B的签名密钥来制作应该对由事务制作部204生成的合约事务数据赋予的签名。这里，设为签名制作部203使用用户B的金密钥来制作金签名。

[0143] 在步骤S205中，终端200的事务制作部204制作被赋予了在步骤S204中制作的签名的合约事务数据。

[0144] 在步骤S206中，终端200的事务制作部204向认证服务器310发送在步骤S205中制作的合约事务数据。

[0145] 认证服务器310在接收在步骤S206中发送的合约事务数据，进行基于正当性验证部303的正当性的验证以及基于信任性验证部302的信任性的验证之后，将合约事务数据储存于分散账本(步骤S101～S104)。

[0146] 根据以上的一系列的处理，信息管理系统1能够具有更高的信任性而在分散账本中管理信息。

[0147] 另外，在上述中，在与条件决定部102所要求的签名的信任度相关的条件中的签名的信任度的规定值也可以在信息管理系统1中预先确定。该情况下，也可以将信任度的规定值设为根据合约事务数据的内容而预先确定的信任度。该情况下，条件决定部102在信息管理系统1中使用根据合约事务数据的内容而预先确定的信任度来决定上述条件。该情况下，数据制作部103制作的合约数据中无需包含要求信任度。

[0148] (实施方式1变形例)

[0149] 在本变形例中，关于具有更高的信任性在分散账本中管理信息信息的管理系统以及其控制方法等，说明与实施方式1不同的方式。在本变形例的信息管理系统中，在从终端100向终端200传递合约内容时，取代合约数据而使用合约事务数据。

[0150] 图9是示出本变形例中的信息管理系统1A的处理的时序图。另外，关于信息管理系统1A的处理中与图8所记载的相同的内容，标注相同的附图标记省略详细的说明。

[0151] 在步骤S211中，终端100的数据制作部103制作表示用户A与用户B之间签订的合约的内容的合约事务数据。数据制作部103制作的合约事务数据取代实施方式1中的合约数据而生成。合约事务数据的内容与实施方式1中的合约数据相同(参照图5)。

[0152] 在步骤S212中，数据制作部103经由通信部104向认证服务器310发送制作的合约事务数据。认证服务器310的账本储存部301接受被发送的合约事务数据。

[0153] 在步骤S213中，认证服务器310将在步骤S212中接收到的合约事务数据储存于分散账本。在将合约数据储存于分散账本时，可以执行共识算法，也可以不执行。

[0154] 在步骤S214中，终端200的合约取得部202向认证服务器310发送合约事务数据的请求。认证服务器310的账本储存部301接收合约事务数据的请求。

[0155] 在步骤S215中，认证服务器310的账本储存部301根据上述接收到的请求，向终端200发送合约事务数据。终端200的合约取得部202接收被发送的合约事务数据。

[0156] 之后，终端200确认接收到的合约事务数据所含的合约内容，基于上述合约内容，生成被赋予了签名的合约事务数据并向认证服务器310发送，使其储存于分散账本(步骤S203～S104)。

[0157] 根据以上的一系列的处理，信息管理系统1A能够具有更高的信任性而在分散账本中管理信息。

[0158] (实施方式2)

[0159] 在本实施方式中，关于具有更高的信任性而在分散账本中管理信息的信息管理系统以及其控制方法等，说明与实施方式1不同的方式。

[0160] 本实施方式的信息管理系统以及信息管理系统所具备的终端100以及200、及认证服务器310、320以及330等与实施方式1中大致相同，但在取代与签名密钥相关联的信任度

而使用与签名密钥相关联的属性这一点上不同。

[0161] 说明本实施方式中的终端100。

[0162] 本实施方式中的终端100与实施方式1中的终端100相同，但条件决定部102以及数据制作部103与实施方式1的终端100中的不同。

[0163] 条件决定部102决定与向用户B要求的签名的属性相关的条件，用户B作为与用户A之间签订合约的对象。与向签订合约的对象要求的签名的属性相关的条件的一个例子是签订合约的对象对合约事务数据赋予的签名的属性包含规定的属性(也称作规定属性)的至少一个这一条件，对这种情况进行说明，但并不限定于此。属性例如是由用户A(也称作要求用户)所确定的、该签名所要求的属性即要求属性。关于属性之后详细地说明，用户A作为向签订合约的对象即用户B要求签名的赋予的用户。

[0164] 数据制作部103制作表示用户A与用户B之间签订的合约的内容的合约数据。数据制作部103取得合约决定部101所决定的合约内容，制作包含合约内容的合约数据。另外，在条件决定部102决定了要求属性作为规定属性的情况下，合约决定部101取得该要求属性，制作包含上述的合约内容与要求属性的合约数据。数据制作部103经由通信部104向终端200发送制作的合约数据。

[0165] 说明本实施方式中的终端200。

[0166] 本实施方式中的终端200与实施方式1的终端200相同，但密钥储存部201以及签名制作部203与实施方式1的终端100中的不同。

[0167] 密钥储存部201具有存储有用户B的签名密钥的存储装置。密钥储存部201中储存有用户B的多个签名密钥。用户B的多个签名密钥各自与属性相关联。这里，属性是指表示用户B的特性或者性质的指标。属性例如表示国籍、住址、年龄、性别、收入状况、债务状况、或者犯罪记录等。

[0168] 签名制作部203是制作用户B的签名的功能部。签名制作部203通过参照事务制作部204制作的合约事务数据，对于合约事务数据进行使用了储存于密钥储存部201的用户B的签名密钥的运算，来制作签名。签名制作部203向事务制作部204提供制作的签名。

[0169] 说明本实施方式中的认证服务器310A。

[0170] 图10是示出本实施方式中的认证服务器310A的功能结构的一个例子的方框图。

[0171] 如图10所示，认证服务器310A具备账本储存部301、属性验证部302A、正当性验证部303、以及通信部304。认证服务器310A所具备的各功能部通过认证服务器310A所具备的CPU(未图示)使用存储器执行规定的程序而实现，此外，可以通过存储装置实现。

[0172] 账本储存部301与实施方式1中的认证服务器310所具备的账本储存部301相同。

[0173] 属性验证部302A是验证合约事务数据的签名的制作所使用的签名密钥的属性的功能部。属性验证部302A取得通过正当性验证部303而验证了正当性的合约事务数据(后述)，通过进行与取得的合约事务数据被赋予的签名的制作所使用的签名密钥相关联的属性(也仅称作“合约事务数据的属性”)是否包含规定属性中的至少一个的判定，来验证合约事务数据的属性。

[0174] 在上述判定中判定为合约事务数据的属性包含规定属性中的至少一个的情况下，属性验证部302A向账本储存部301提供合约事务数据并使其储存于分散账本。此外，在上述判定中判定为合约事务数据的属性不包含规定属性中的至少一个的情况下，属性验证部

302A执行使合约事务数据无效的无效化处理。关于无效化处理与上述实施方式1中的情况相同。

[0175] 在属性验证部302A的判定中，也可以使用“全部的规定属性”作为“规定属性中的至少一个”。即，也可以是，属性验证部302A通过进行被赋予给取得的合约事务数据的签名的制作所使用的签名密钥的属性是否包含全部的规定属性的判定，来验证合约事务数据的属性。在这种情况下，属性验证部302A在上述判定中判定为合约事务数据的属性包含全部的规定属性的情况下，向账本储存部301提供合约事务数据并使其储存于分散账本。此外，属性验证部302A在上述判定中判定为合约事务数据的属性不包含全部的规定属性含的情况下，执行使合约事务数据无效的无效化处理。

[0176] 正当性验证部303与实施方式1中的正当性验证部303相同。正当性验证部303接收到的合约事务数据包含要求属性。正当性验证部303向属性验证部302A提供验证了正当的、即验证处理成功了的合约事务数据。

[0177] 另外，在合约事务数据中包含合约的签订者即用户A以及B双方的签名的情况下，正当性验证部303分别使用双方的签名进行验证处理。

[0178] 图11是示出本实施方式中的合约数据的一个例子的说明图。

[0179] 如图11所示，合约数据包含签订者1以及2合约内容、要求属性、及签名1以及2的字段。合约数据由合约决定部101制作。在合约数据所含的字段中，除要求属性与签名1以及2以外的字段与实施方式1中的相同，因此省略说明。

[0180] 要求属性是该合约所要求的签名密钥的属性。要求属性，例如是用户A向用户B要求的签名的制作所使用的签名密钥的属性。图11所示要求属性中，国籍的属性为“日本”，年代的属性为“30代”，性别的属性为“男性”。

[0181] 签名1是该合约数据的合约的签订者中的一个合约者的签名。在用户A销售商品的买卖合约中，在合约数据被制作的时刻，决定了签订者中的一个合约者为用户A，因此，签名1被赋予用户A的签名S。在与签名S的制作所使用的签名密钥(也称作“签名S的签名密钥”)相关联的属性中，国籍的属性为“日本”，年代的属性为“30代”，性别的属性为“男性”。

[0182] 签名2是该合约数据的合约的签订者中的除签订者以外的一个合约者的签名。在图11中，以签订者2未决定的情况为一个例子示出，示出了签名2尚未被赋予这一情况。

[0183] 图12是示出本实施方式中的合约事务数据的一个例子的说明图。

[0184] 如图12所示，合约事务数据包含签订者1以及2合约内容、要求属性、及签名1以及2的字段。合约事务数据由事务制作部204制作。合约数据所含的字段中的要求属性以外的字段与实施方式1中的相同，因此省略说明。此外，要求属性的字段与合约数据中的相同，因此省略说明。

[0185] 在合约事务数据被制作的时刻，签订者中的除用户A以外的一方决定为用户B，因此，签订者2以及签名2的字段与合约数据中的不同。

[0186] 在合约事务数据被制作的时刻，用户A以及B的双方被确定。在生成合约事务数据的时刻，签订者2被确定为用户B，从而签订者2包含用户B的识别信息，签名2包含用户B的签名T。在与签名T的制作所使用的签名密钥(也称作“签名T的签名密钥”)相关联的属性中，国籍的属性为“日本”，年代的属性为“30代”，性别的属性为“男性”。

[0187] 图13是示出本实施方式中的认证服务器310A的处理的流程图。

[0188] 图13所示的处理中的步骤S103A以外的处理与实施方式1中的相同。

[0189] 在步骤S103A中，属性验证部302A判定被赋予给在步骤S102中判定为正当的合约事务数据的签名的制作所使用的签名密钥的属性是否包含规定属性中的至少一个。在判定为签名密钥的属性包含规定属性中的至少一个的情况下(步骤S103A中的是)，进入步骤S104，在相反的情况下(步骤S103A中的否)，进入步骤S121。

[0190] 本实施方式的信息管理系统的处理通过将实施方式1中的信息管理系统1的处理(图8)的步骤S103置换为图13的步骤S103A而说明。省略详细的说明。

[0191] 根据图13所示的一系列的处理，信息管理系统能够具有更高的信任性而在分散账本中管理信息。

[0192] 另外，在上述中，与条件决定部102所要求的签名的属性相关的条件中的签名的规定属性也可以在信息管理系统中被预先确定。该情况下，信任度的规定属性也可以作为根据合约事务数据的内容而预先确定的属性。该情况下，条件决定部102使用在信息管理系统中根据合约事务数据的内容而预先确定的属性来决定上述条件。该情况下，数据制作部103制作的合约数据无需包含要求属性。

[0193] 此外，在上述中，按每个属性设定一个属性值作为要求属性，但也可以设定多个属性值作为要求属性。在这种情况下，属性验证部302A判定被赋予给合约事务数据的签名的制作所使用的签名密钥的属性是否包含规定属性中的至少一个属性值。例如，也可以是，在要求属性所含的国籍的属性为“日本”或者“美国”的情况下，无论与签名密钥相关联的国籍的属性为“日本”或者“美国”中的哪一个，均判定为签名密钥的属性包含规定属性。

[0194] 此外，也可以设定将多个属性的属性值组合的条件作为要求属性。例如，也可以是，如国籍为“日本”并且年龄为“30代”，或者国籍为“美国”并且年龄为“40代”这样，设定将国籍的属性与年龄的属性组合的条件。在这种情况下，属性验证部302A在将多个属性的属性值组合的条件满足的情况下，判定为签名密钥的属性包含规定属性。

[0195] (补充)

[0196] 对上述各实施方式或者变形例的区块链进行补充说明。

[0197] 图14是示出区块链的数据构的说明图。

[0198] 区块链通过作为其记录单位的区块被以链(chain)状连接而成。各个区块具有多个事务数据以及紧前的区块的哈希值。具体而言，区块B2中包含之前的区块B1的哈希值。并且，根据区块B2中包含的多个事务数据以及区块B1的哈希值而运算出的哈希值作为区块B2的哈希值而包含于区块B3中。如此，包含之前的区块的内容作为哈希值，并且，以链状连接区块，从而有效地防止记录的事务数据的篡改。

[0199] 假设若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，要想使篡改后的区块伪装成正确的区块，必须重新制作其后的全部区块，该作业在现实中非常困难。利用该性质，在区块链中确保了篡改困难性。

[0200] 图15是示出事务数据的数据构造的说明图。

[0201] 图15所示的事务数据包含事务主体P1以及电子签名P2。事务主体P1是该事务数据所含的数据主体。电子签名P2是通过对于事务主体P1的哈希值，由该事务数据的制作者的签名密钥进行签名，更具体而言由制作者的秘密密钥进行加密而生成的签名。

[0202] 事务数据具有电子签名P2，因此篡改在实质上是不可能的。由此，防止了事务主体

的篡改。

[0203] 另外，在上述实施方式中，也可以是，各结构要素由专用的硬件构成，或者通过执行适合各结构要素的软件程序来实现。也可以是，各结构要素通过CPU或者处理器等程序执行部读出并执行记录于硬盘或者半导体存储器等记录介质中的软件程序来实现。这里，实现上述实施方式的内容管理系统等的软件是如下的程序。

[0204] 即，该程序使计算机执行以下控制方法，所述控制方法是在具备保有分散账本的多个服务器的信息管理系统中，该多个服务器中的一个服务器所执行的控制方法，在所述控制方法中，接收包含使用信任度与后述多个签名密钥分别相关联的多个签名密钥中的某签名密钥而制作的签名的事务数据，所述多个签名密钥是用户所保有的多个签名密钥，进行与接收到的所述事务数据中包含的所述签名的制作所使用的所述签名密钥相关联的所述信任度是否为规定值以上的判定，在所述判定中判定为所述信任度为所述规定值以上的情况下，将所述事务数据储存于所述分散账本，在所述判定中判定为所述信任度小于所述规定值的情况下，执行使所述事务数据无效的无效化处理。

[0205] 以上，对于一个或多个形态所涉及的合约管理系统等，基于实施方式进行了说明，但是，本发明并不限于该实施方式。只要不脱离本发明的主旨，本领域技术人员对本实施方式执行想到的各种变形，或组合不同的实施方式的构成要素来构成的方式，也可以包含在一个或多个形态的范围内。

[0206] 产业上的可利用性

[0207] 本发明能够利用于管理各种信息的信息管理系统。

[0208] 附图标记说明

[0209] 1、1A 信息管理系统

[0210] 100、200 终端

[0211] 101 合约决定部

[0212] 102 条件决定部

[0213] 103 数据制作部

[0214] 104、205、304 通信部

[0215] 201 密钥储存部

[0216] 202 合约取得部

[0217] 203 签名制作部

[0218] 204 事务制作部

[0219] 301 账本储存部

[0220] 302 信任性验证部

[0221] 302A 属性验证部

[0222] 303 正当性验证部

[0223] 310、310A、320、330 认证服务器

[0224] A、B 用户

[0225] B1、B2、B3 区块

[0226] P1 事务主体

[0227] P2 电子签名

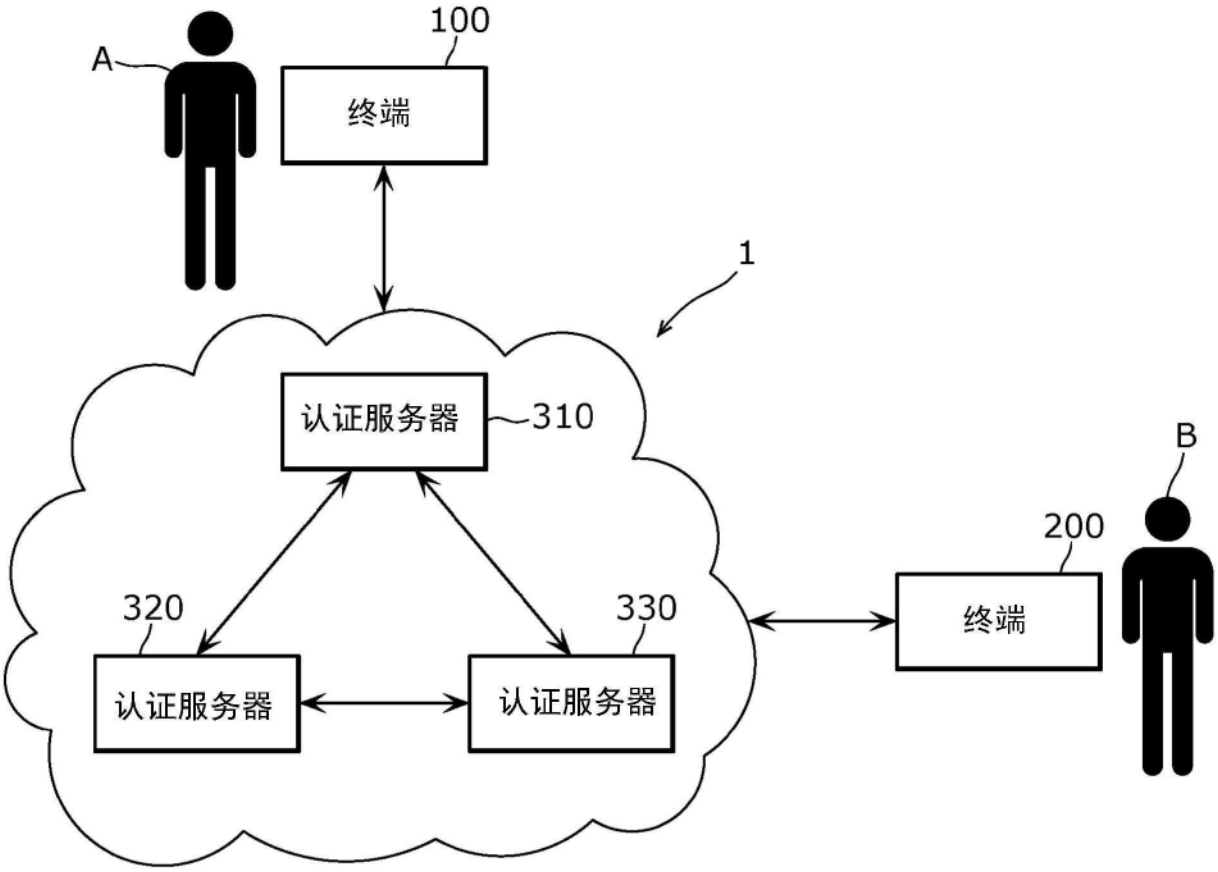

100
A
终端
1
认证服务器
310
B
200
320
330
终端
认证服务器
认证服务器

图1

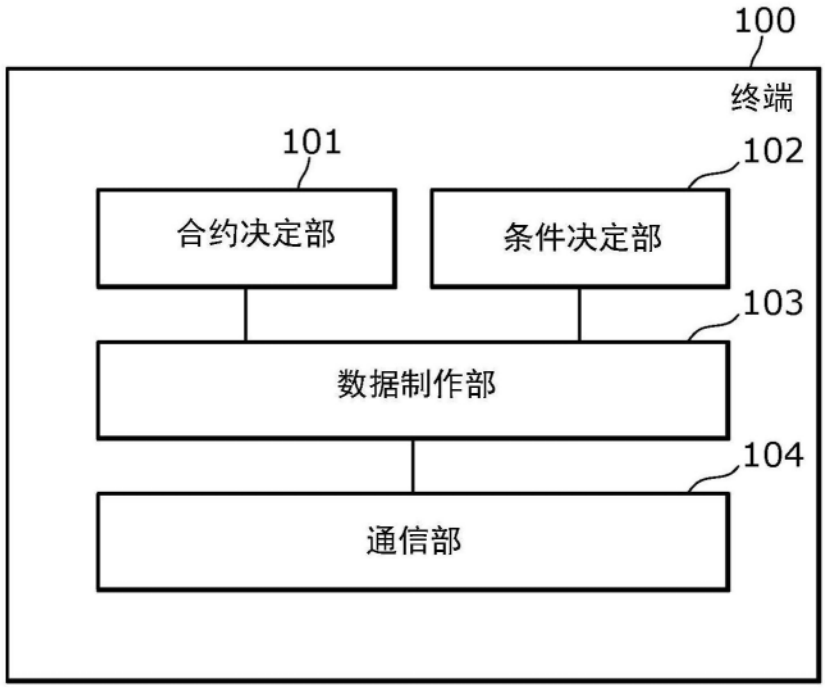

100
终端
101
102
合约决定部
条件决定部
103
数据制作部
104
通信部

图2

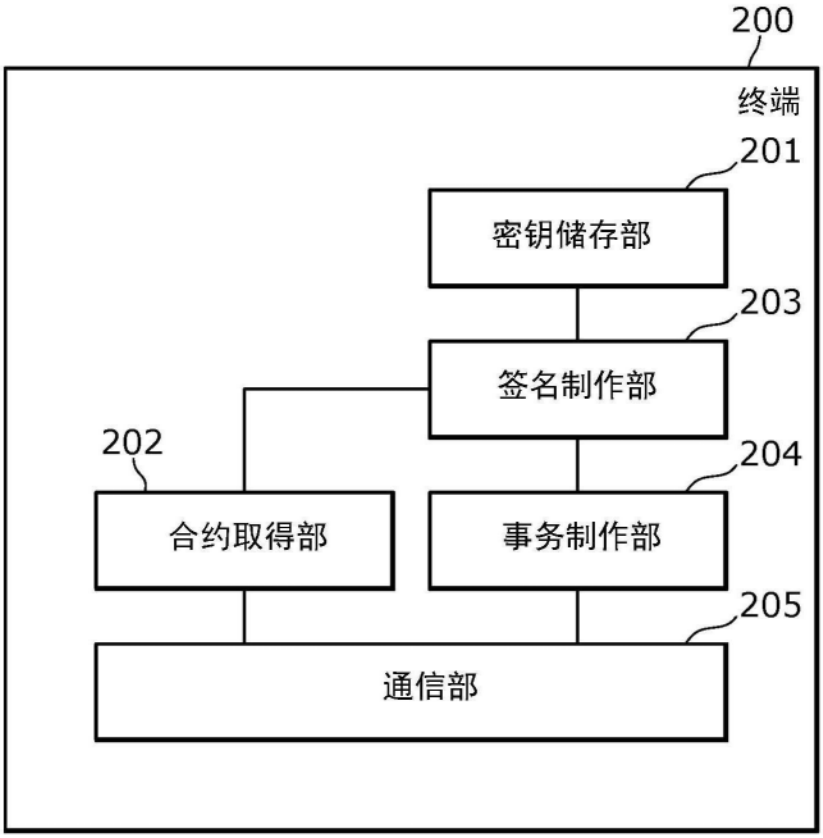


图3

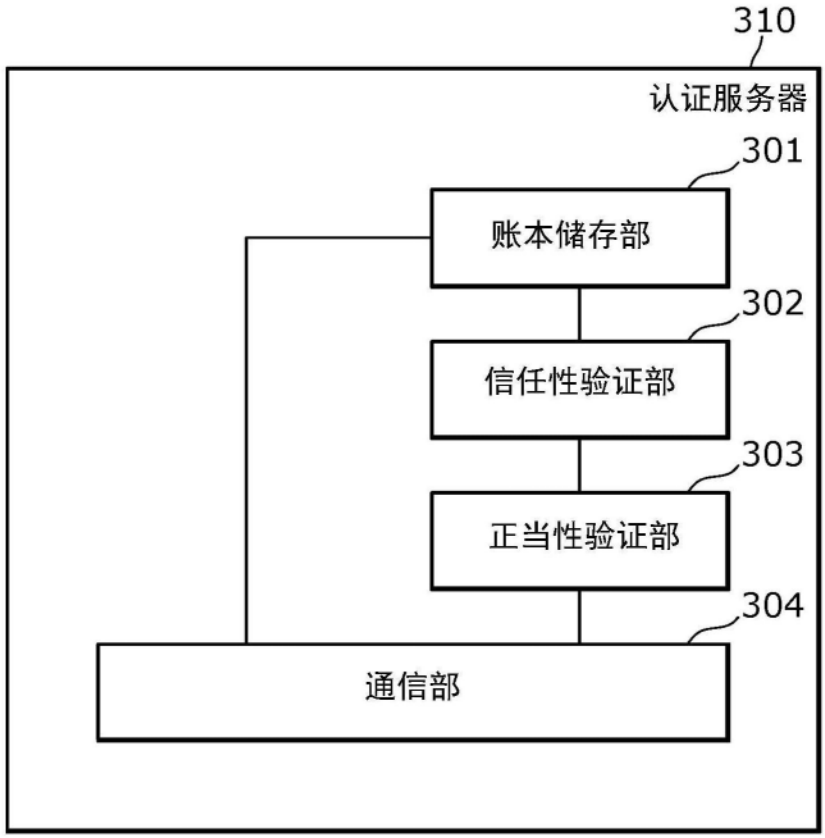


图4

签订者1	签订者2	合约内容	要求信任度
用户A	（待定）	商品编号=A001、数量=100、 交付日期=2020/2/1、价格=￥10，000	金

签名1	签名2
用户A的 金签名	-

图5

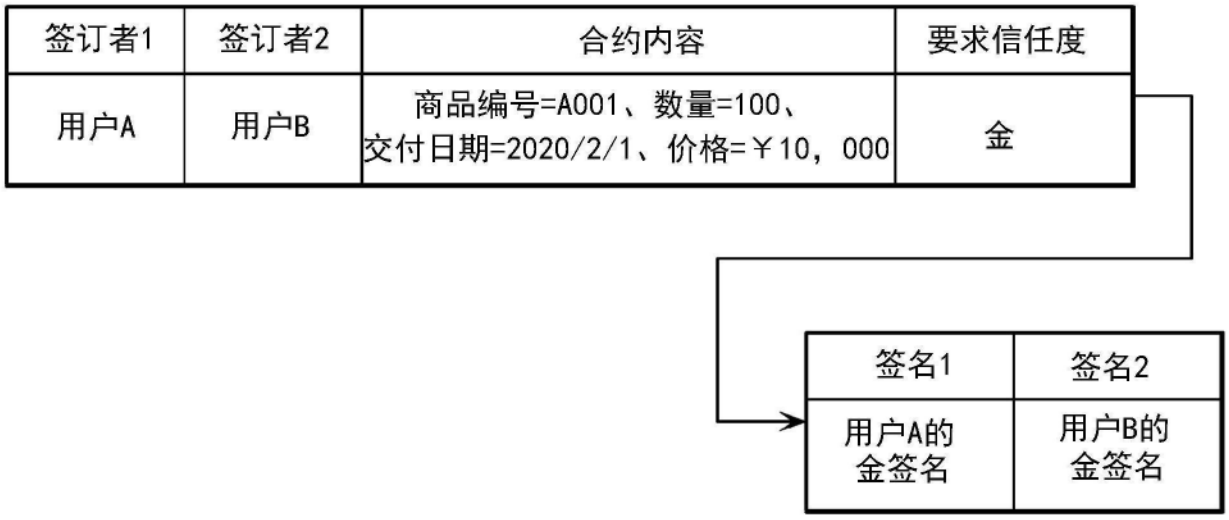

签订者1
签订者2
合约内容
要求信任度
用户A
用户B
商品编号=A001、数量=100、
交付日期=2020/2/1、价格=￥10，000
金
签名1
签名2
用户A的
金签名
用户B的
金签名

图6

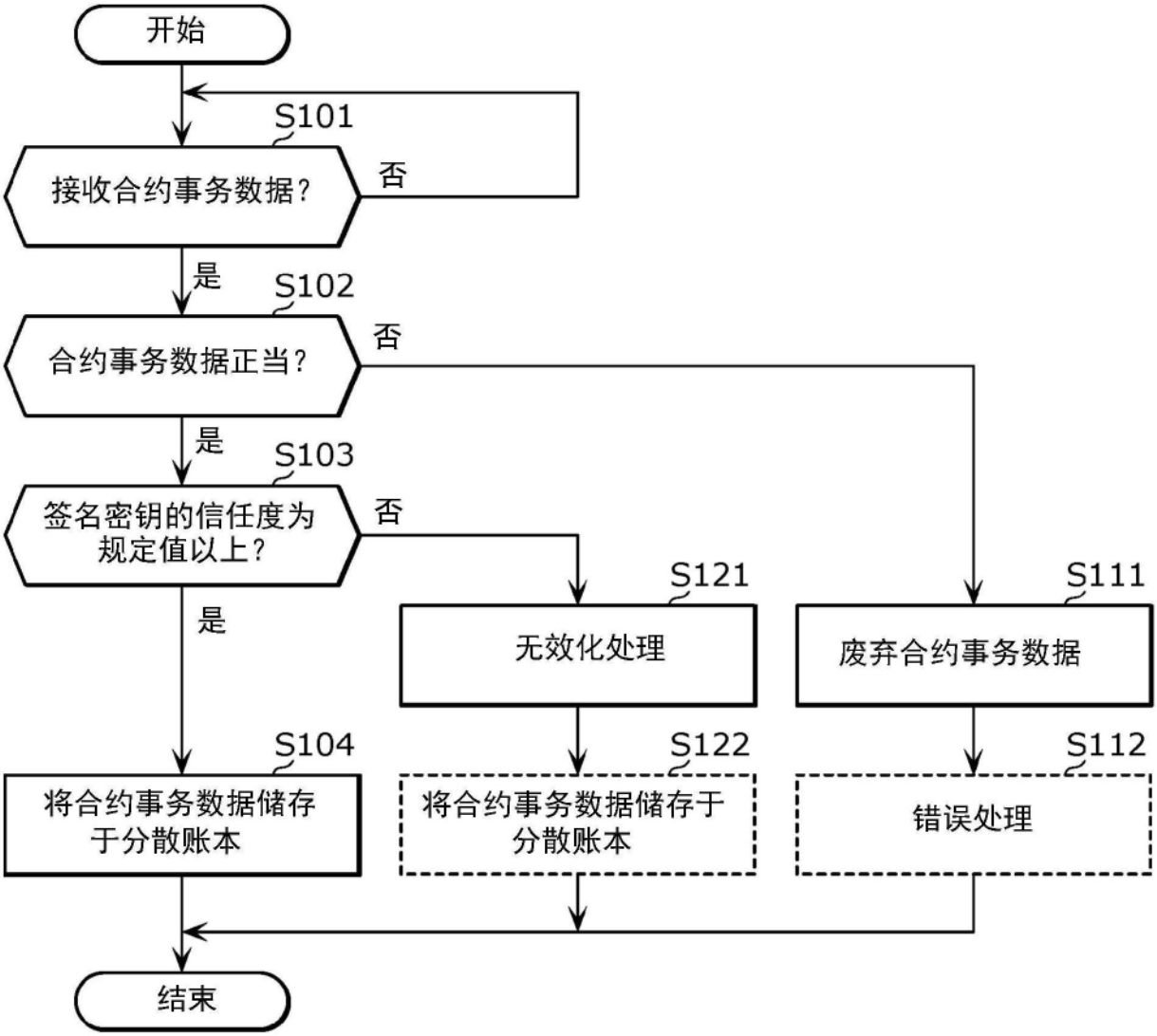

开始
S101
接收合约事务数据？
否
是
S102
合约事务数据正当？
否
是
S103
签名密钥的信任度为规定值以上？
否
是
S121
无效化处理
S111
废弃合约事务数据
S104
将合约事务数据储存于分散账本
S122
将合约事务数据储存于分散账本
S112
错误处理
结束

图7

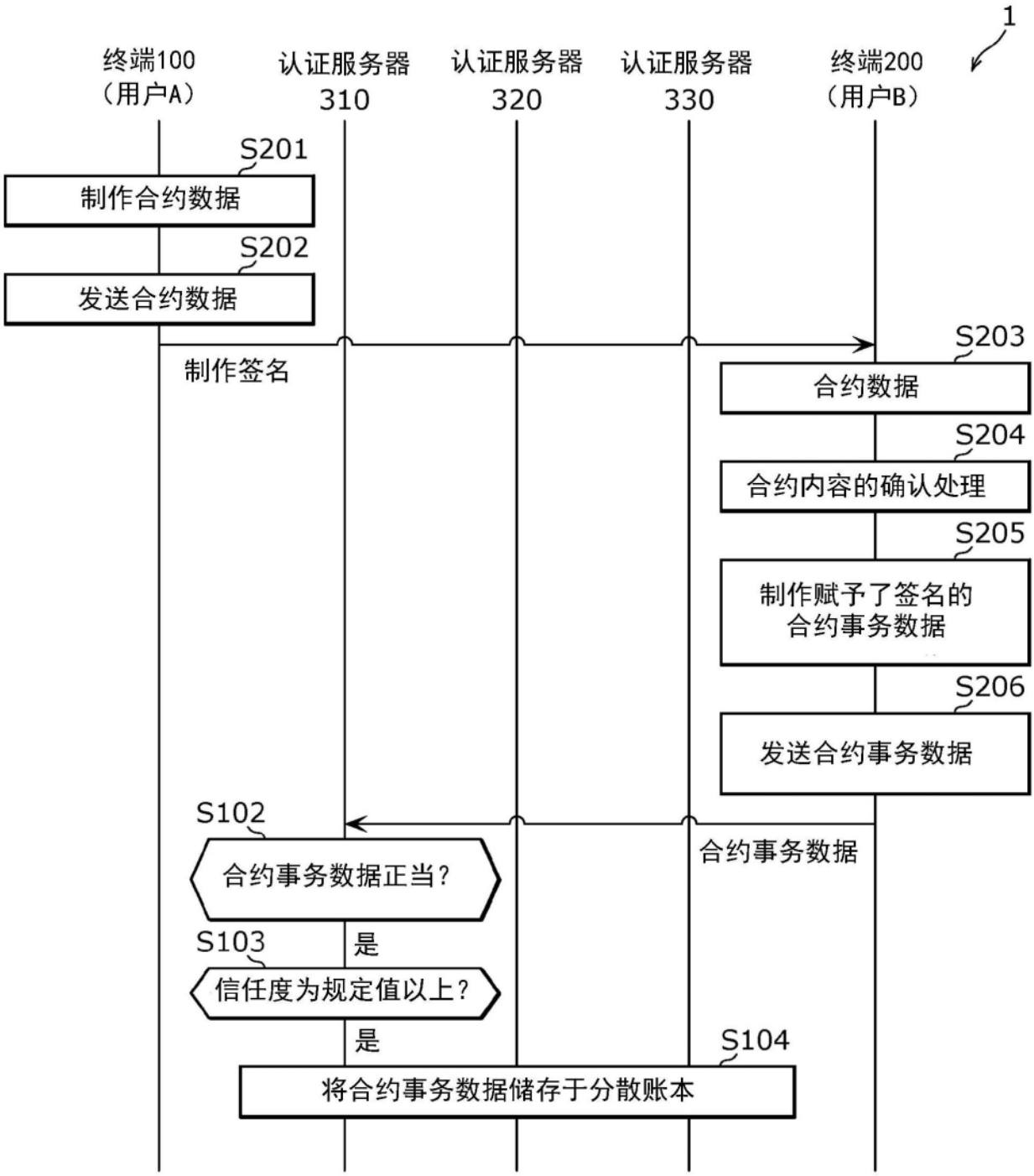

1
终端100
（用户A）
认证服务器
310
认证服务器
320
认证服务器
330
终端200
（用户B）
S201
制作合约数据
S202
发送合约数据
制作签名
S203
合约数据
S204
合约内容的确认处理
S205
制作赋予了签名的
合约事务数据
S206
发送合约事务数据
S102
合约事务数据正当？
合约事务数据
S103
是
信任度为规定值以上？
是
S104
将合约事务数据储存于分散账本

图8

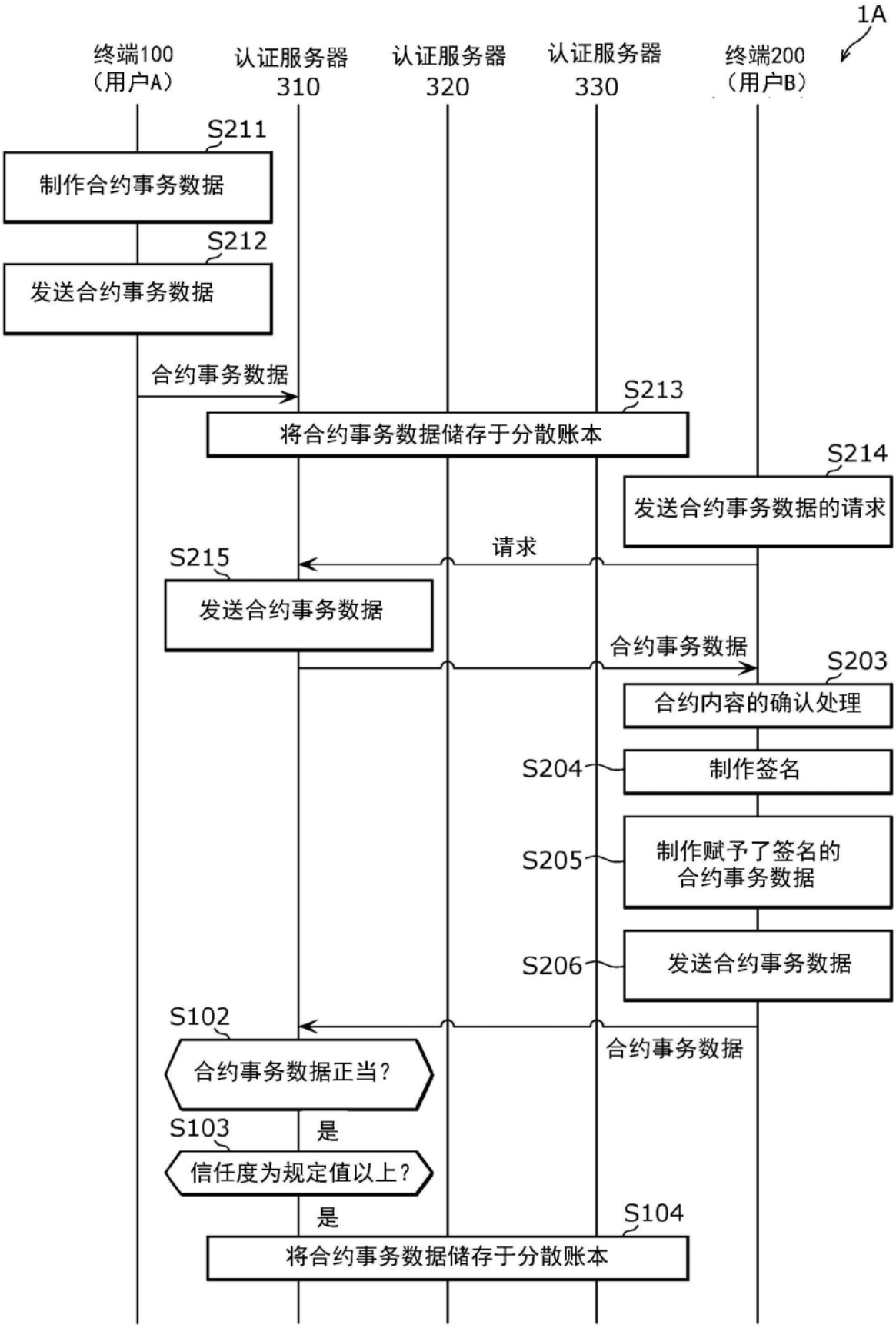

1A
终端100
（用户A）
认证服务器
310
认证服务器
320
认证服务器
330
终端200
（用户B）
S211
制作合约事务数据
S212
发送合约事务数据
合约事务数据
S213
将合约事务数据储存于分散账本
S214
发送合约事务数据的请求
请求
S215
发送合约事务数据
合约事务数据
S203
合约内容的确认处理
S204
制作签名
S205
制作赋予了签名的
合约事务数据
S206
发送合约事务数据
S102
合约事务数据
合约事务数据正当？
S103
是
信任度为规定值以上？
是
S104
将合约事务数据储存于分散账本

图9

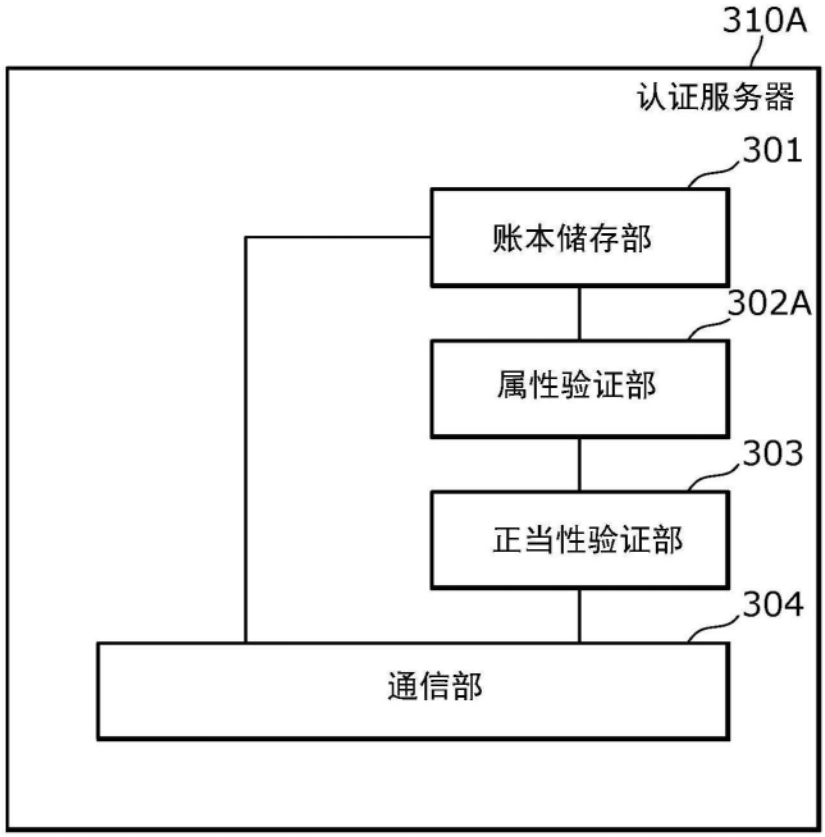


图10

签订者1	签订者2	合约内容
用户A	（待定）	商品编号=A001、数量=100、 交付日期=2020/2/1、价格=￥10，000

要求属性	签名1	签名2
国籍=日本、年代=30代、性别=男性	用户A的签名S	–

与签名S的签名密钥相关的属性
：日本人、30代、男性

图11

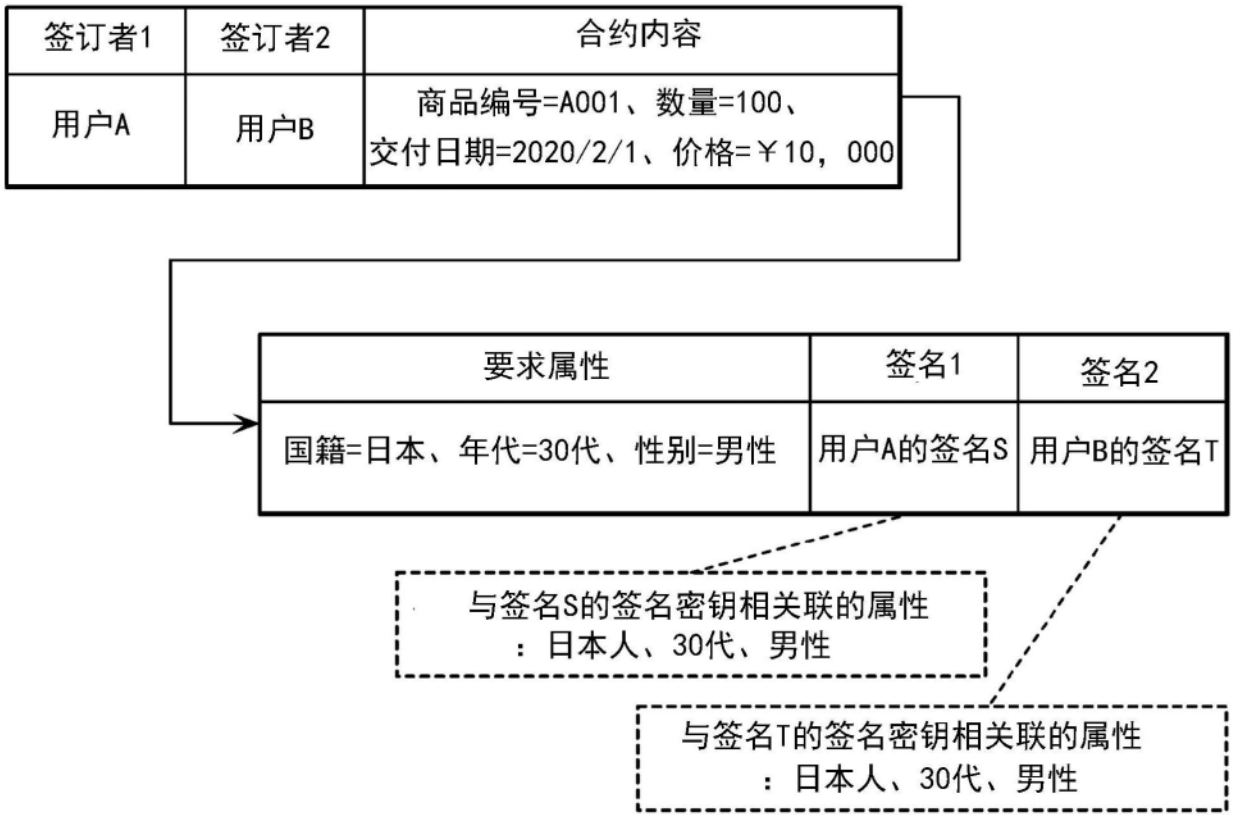

签订者1
签订者2
合约内容
用户A
用户B
商品编号=A001、数量=100、
交付日期=2020/2/1、价格=￥10，000
要求属性
签名1
签名2
国籍=日本、年代=30代、性别=男性
用户A的签名S
用户B的签名T
与签名S的签名密钥相关联的属性
：日本人、30代、男性
与签名T的签名密钥相关联的属性
：日本人、30代、男性

图12

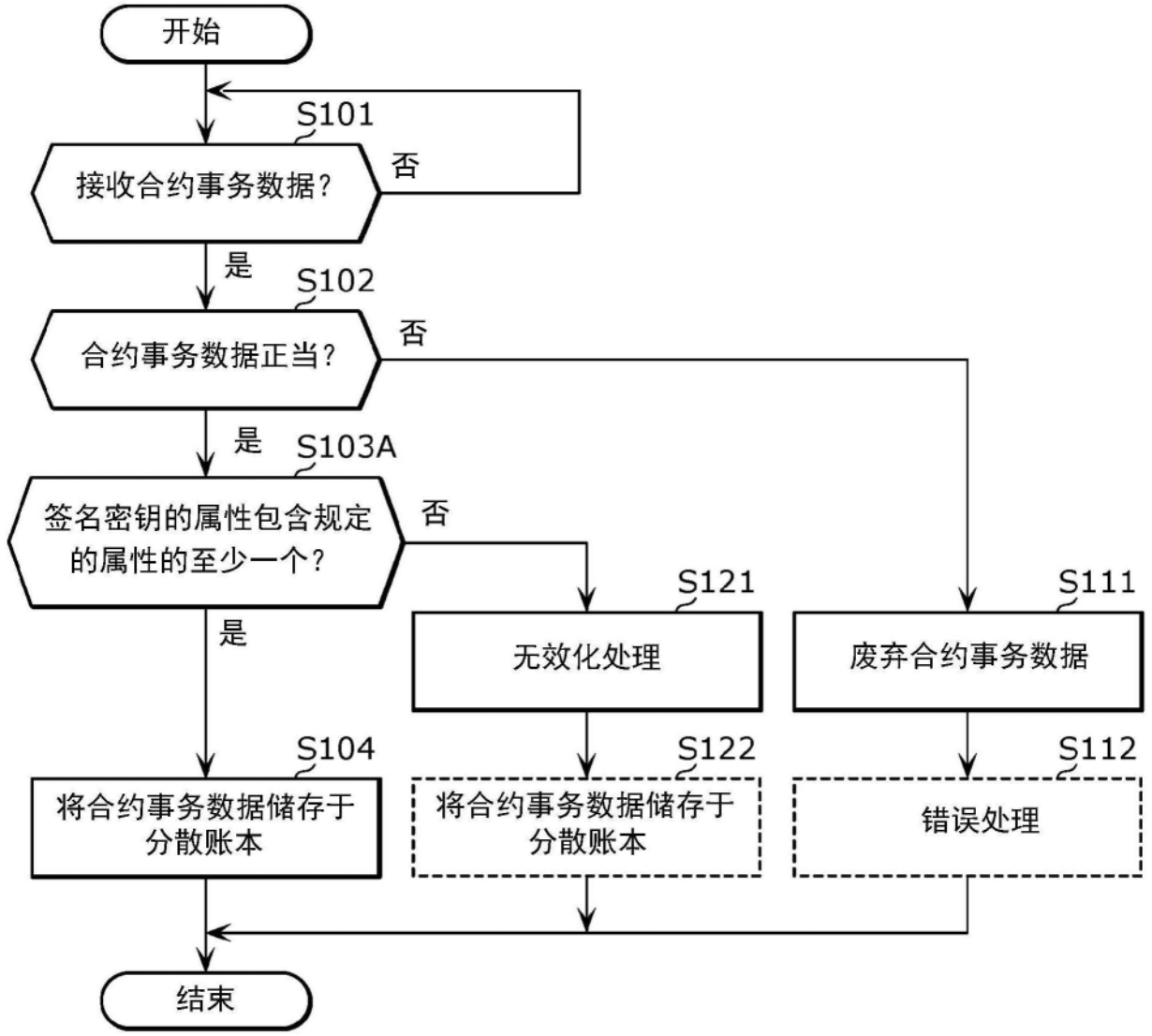

开始
S101
接收合约事务数据?
否
是
S102
合约事务数据正当?
否
是
S103A
签名密钥的属性包含规定的属性的至少一个?
否
是
S121
无效化处理
S111
废弃合约事务数据
S104
将合约事务数据储存于分散账本
S122
将合约事务数据储存于分散账本
S112
错误处理
结束

图13

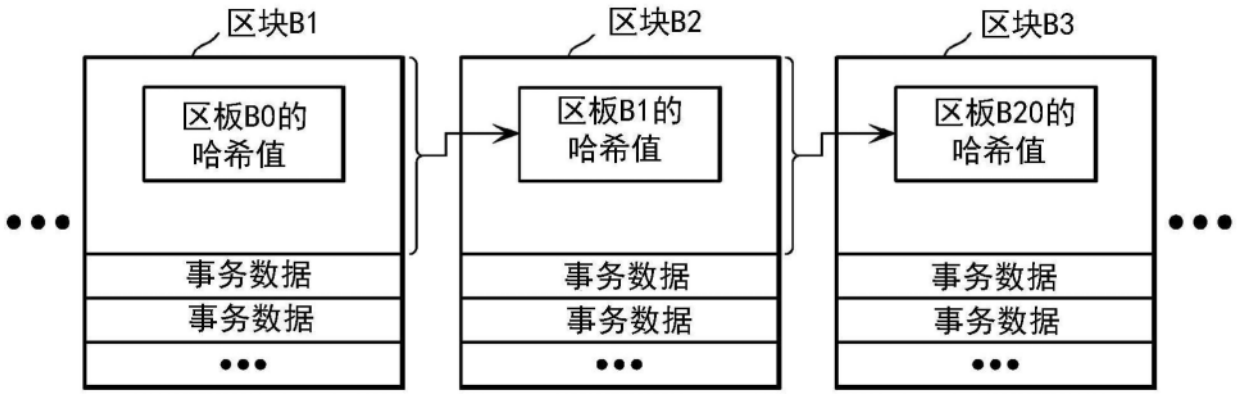

区块B1
区板B0的哈希值
事务数据
事务数据
区块B2
区板B1的哈希值
事务数据
事务数据
区块B3
区板B20的哈希值
事务数据
事务数据

图14

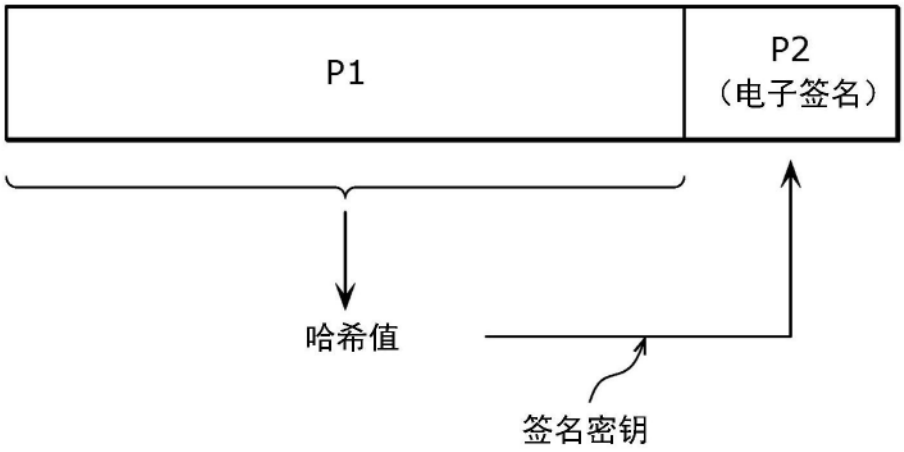


图15