(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 110235410 B
(45)授权公告日 2022.05.10

(21)申请号 201880006807.2
(22)申请日 2018.01.19
(65)同一申请的已公布的文献号
申请公布号 CN 110235410 A
(43)申请公布日 2019.09.13
(30)优先权数据
10-2017-0019770 2017.02.14 KR
(85)PCT国际申请进入国家阶段日
2019.07.12
(86)PCT国际申请的申请数据
PCT/KR2018/000912 2018.01.19
(87)PCT国际申请的公布数据
WO2018/151425 KO 2018.08.23
(73)专利权人 科因普拉格株式会社
地址 韩国京畿道
(72)发明人 罗承一 金熙淳 洪载佑 鱼浚善
(74)专利代理机构 北京同立钧成知识产权代理有限公司 11205
专利代理师 王蕊 臧建明
(51)Int.Cl.
H04L 9/32(2006.01)
(56)对比文件
CN 107454077 A,2017.12.08
CN 106375270 A,2017.02.01
KR 101628004 B1,2016.06.08
KR 101085631 B1,2011.11.22
KR 101661933 B1,2016.10.05
审查员 陈静

权利要求书8页 说明书24页 附图6页

(54)发明名称

使用基于UTXO的协议的区块链数据库并通过基于PKI的认证取代用户的登录的方法及利用其的服务器

(57)摘要

根据本发明,提供使用区块链数据库通过基于PKI的认证取代针对用户的登录请求的登录的方法。根据本发明的方法,如果从在用户终端执行的服务提供应用程序中获得通过认证应用程序取代登录的请求的认证请求信息,则服务提供服务器向上述服务提供应用程序传递认证请求响应信息,并在其认证重定向请求传递至上述认证应用程序后,如果获得服务器质询请求信息,则向上述认证应用程序传递服务器质询请求响应信息,从认证服务器获得包含上述服务器及上述应用程序的认证书是否有效的认证结果消息,并且,向上述服务提供应用程序传递预定的访问令牌,以处理上述登录使得能够利用上述服务。

CN 110235410 B

1.一种方法,其为使用区块链数据库通过基于公钥基础设施PKI(public key infrastructure)的认证取代针对利用服务提供服务器所提供的服务的用户的登录请求的登录的方法,其特征在于,包括:

步骤(a),上述服务提供服务器,在作为利用通过基于上述PKI的加密方式生成的服务器公钥和服务器私钥的上述服务提供服务器的认证书的服务器认证书的信息或者作为对此进行加工后的值的服务器认证书注册事务及作为利用通过基于上述PKI的加密方式生成的应用程序公钥和应用程序私钥的认证应用程序的认证书的应用程序认证书的信息或者作为对此进行加工后的值的应用程序认证书注册事务被记录于上述区块链数据库的状态,从用户终端所执行的服务提供应用程序中获得作为请求通过上述用户终端所执行的上述认证应用程序取代登录的信息的认证请求信息,向上述服务提供应用程序传递作为判断是否能够取代上述登录的结果的认证请求响应信息;

步骤(b),上述服务提供服务器从上述认证应用程序获得包含可变认证值的服务器质询请求信息,上述可变认证值为通过上述认证应用程序接收根据来自上述服务提供应用程序的认证重定向请求(authentication redirection request)的质询开始请求信息的认证服务器生成的与上述质询开始请求信息对应的可变认证值,向上述认证应用程序传递与上述服务器质询请求信息相对应的服务器质询请求响应信息,通过上述认证应用程序向上述认证服务器传递响应请求信息,从而支援上述认证服务器利用上述区块链数据库中记录的上述服务器认证书注册事务和上述应用程序认证书注册事务确认上述响应请求信息,判断上述服务器认证书及上述应用程序认证书是否有效;以及

步骤(c),上述服务提供服务器获得来自上述认证服务器的包含上述服务器认证书及上述应用程序认证书是否有效的认证结果消息,如果上述认证结果消息为表示上述服务器认证书及上述应用程序认证书有效的认证成功消息,则向上述服务提供应用程序传递预定的访问令牌(access token),从而支援上述服务提供应用程序能够通过上述访问令牌利用上述服务,由此对上述登录进行处理。

2.根据权利要求1所述的方法,其特征在于,在上述步骤(b)中,上述服务器质询请求信息包含被与上述服务器认证书对应的上述服务器公钥所编码的上述可变认证值,上述服务提供服务器利用与上述服务器认证书对应的上述服务器私钥从上述服务器质询请求信息中获得上述可变认证值,并向上述认证应用程序传递上述服务器质询请求响应信息,其中,上述服务器质询请求响应信息包含利用上述服务器私钥对上述可变认证值进行签名的值。

3.根据权利要求1所述的方法,其特征在于,上述区块链数据库为私人区块链数据库或者公共区块链数据库。

4.一种方法,其为使用区块链数据库通过基于公钥基础设施PKI(public key infrastructure)的认证取代针对利用服务提供服务器所提供的服务的用户的登录请求的登录的方法,其特征在于,包括:

步骤(a),认证服务器,在作为利用通过基于上述PKI的加密方式生成的服务器公钥和服务器私钥的上述服务提供服务器的认证书的服务器认证书的信息或者作为对此进行加工后的值的服务器认证书注册事务及作为利用通过基于上述PKI的加密方式生成的应用程序公钥和应用程序私钥的认证应用程序的认证书的应用程序认证书的信息或者作为对此进行加工后的值的应用程序认证书注册事务被记录于上述区块链数据库的状态,响应与作

为请求通过用户终端所执行的认证应用程序取代登录的信息的认证请求信息相对应的认证重定向请求(authentication redirection request),从通过上述用户终端执行的认证应用程序中获得质询开始请求信息,生成与上述质询开始请求信息相对应的可变认证值,向上述认证应用程序传递包含上述可变认证值的质询开始请求响应信息,从而使上述认证应用程序从上述服务提供服务器获得服务器质询请求响应信息,上述服务器质询请求响应信息与用于判断上述服务器认证书是否有效的服务器质询请求信息相对应;

步骤(b),上述认证服务器,利用与上述应用程序认证书对应的上述应用程序私钥从上述认证应用程序中获得包含作为对上述服务器质询请求响应信息进行签名的值的多重签名值的响应请求信息,利用上述区块链数据库中记录的上述服务器认证书注册事务和上述应用程序认证书注册事务确认上述响应请求信息,判断上述服务器认证书及上述应用程序认证书是否有效;以及

步骤(c),上述认证服务器向上述认证应用程序及上述服务提供服务器中的至少一个传递包含上述服务器认证书是否有效的认证结果消息,从而在上述认证结果消息为表示上述服务器认证书有效的认证成功消息的情况下,支援上述服务提供服务器向通过上述用户终端执行的服务提供应用程序传递预定的访问令牌(access token),由此支援上述服务提供应用程序能够通过上述访问令牌利用上述服务,由此对上述登录进行处理。

5.根据权利要求4所述的方法,其特征在于,上述认证服务器管理与针对上述服务提供服务器的访问级别(accesslevel)相关的信息,或者支援进行管理,并参照上述访问级别决定授权级别(authorizationlevel),上述认证结果消息包含与上述授权级别相关的信息,其中上述服务器认证书是否有效则参照上述授权级别进行判断。

6.根据权利要求4所述的方法,其特征在于,在上述步骤(b)中,利用与上述服务器认证书对应的上述服务器公钥及与上述应用程序认证书对应的上述应用程序公钥对上述多重签名值的签名进行验证,从而判断上述服务器认证书及上述应用程序认证书是否有效。

7.根据权利要求4所述的方法,其特征在于,在进行上述步骤(b)之后,还包括步骤(c0),上述认证服务器将上述认证结果消息或者对此进行加工的值作为认证结果事务记录于上述区块链数据库。

8.根据权利要求4所述的方法,其特征在于,还包括步骤(d),上述认证服务器响应周期性(periodically)或者完整性验证请求,参照上述区块链数据库所记录的(I)服务器认证书的信息或者作为对此进行加工后的值的服务器认证书注册事务,(II)应用程序认证书的信息或者作为对此进行加工后的值的应用程序认证书注册事务,以及(III)认证结果消息或者作为对此进行加工后的值的认证结果事务中的至少一个信息验证上述(I)、(II)、(III)的信息的完整性(integrity)。

9.一种方法,其为使用区块链数据库通过基于公钥基础设施PKI(public key infrastructure)的认证取代针对利用服务提供服务器所提供的服务的用户的登录请求的登录的方法,其特征在于,包括:

步骤(a),上述服务提供服务器,在作为利用通过基于上述PKI的加密方式生成的服务器公钥和服务器私钥的上述服务提供服务器的认证书的服务器认证书的信息或者作为对此进行加工后的值的服务器认证书注册事务及作为利用通过基于上述PKI的加密方式生成的应用程序公钥和应用程序私钥的第二应用程序的认证书的应用程序认证书的信息或者

作为对此进行加工后的值的应用程序认证书注册事务被记录于上述区块链数据库的状态，从上述第二应用程序获得包含与作为请求通过用户终端所执行的上述第二应用程序取代登录的信息的来自通过上述用户终端执行的第一应用程序的认证重定向请求(authentication redirection request)对应的用于识别上述用户的用户识别信息的认证请求信息，向认证服务器传递包含上述用户识别信息的质询开始请求信息；

步骤(b)，上述服务提供服务器，响应上述质询开始请求信息获得包含由上述认证服务器生成的可变认证值的质询开始请求响应信息，向上述第二应用程序传递包含上述可变认证值的应用程序质询请求信息，从而支援上述第二应用程序生成利用与上述应用程序认证书对应的上述应用程序私钥对上述可变认证值进行签名的值；

步骤(c)，上述服务提供服务器，获得包含利用上述应用程序私钥进行签名的值的应用程序质询请求响应信息，向上述认证服务器传递上述应用程序质询请求响应信息，从而支援上述认证服务器利用上述区块链数据库中记录的上述应用程序认证书注册事务确认上述应用程序质询请求响应信息，判断上述应用程序认证书是否有效；以及

步骤(d)，上述服务提供服务器，从上述认证服务器中获得包含上述应用程序认证书是否有效的认证结果消息，上述认证结果消息为表示上述应用程序认证书有效的认证成功消息，向上述第二应用程序传递临时ID(temporaryID)，并支援上述第一应用程序能够通过从上述第二应用程序向上述第一应用程序传递的(i)上述临时ID及(ii)上述认证成功消息所包含的访问令牌(access token)利用上述服务，由此对上述登录进行处理。

10.根据权利要求9所述的方法，其特征在于，上述质询开始请求信息还包括与上述服务器认证书对应的上述服务器公钥，上述质询开始请求响应信息包含通过上述服务器公钥编码的上述可变认证值，其中，在上述步骤(b)中，上述服务提供服务器利用与上述服务器认证书对应的上述服务器私钥从上述质询开始请求响应信息中获得上述可变认证值，并利用与上述应用程序认证书对应的上述应用程序公钥向上述第二应用程序传递包含对上述可变认证值进行签名的值的上述应用程序质询请求信息。

11.根据权利要求9所述的方法，其特征在于，上述临时ID参照上述认证成功消息所包含的访问令牌(access token)及与授权级别相关的信息决定。

12.一种方法，其为使用区块链数据库通过基于公钥基础设施PKI(public key infrastructure)的认证取代针对利用服务提供服务器所提供的服务的用户的登录请求的登录的方法，其特征在于，包括：

步骤(a)，认证服务器，在作为利用通过基于上述PKI的加密方式生成的服务器公钥和服务器私钥的上述服务提供服务器的认证书的服务器认证书的信息或者作为对此进行加工后的值的服务器认证书注册事务及作为利用通过基于上述PKI的加密方式生成的应用程序公钥和应用程序私钥的第二应用程序的认证书的应用程序认证书的信息或者作为对此进行加工后的值的应用程序认证书注册事务被记录于上述区块链数据库的状态，从上述服务提供服务器获得包含上述用户识别信息的质询开始请求信息，其中，上述服务提供服务器从用户终端所执行的第一应用程序中获得包含用于从接收作为通过上述用户终端所执行的上述第二应用程序请求取代登录的信息的认证重定向请求(authentication redirection request)的上述第二应用程序中识别上述用户的用户识别信息的认证请求信息，响应上述质询开始请求信息生成可变认证值；

步骤(b),上述认证服务器,向上述服务提供服务器传递包含所生成的上述可变认证值的质询开始请求响应信息,从而支援上述服务提供服务器向上述第二应用程序传递包含上述可变认证值的应用程序质询请求信息,由此支援上述第二应用程序生成利用与上述应用程序认证书对应的应用程序私钥(private key)对上述可变认证值进行签名的值;

步骤(c),上述认证服务器,获得包含利用与上述应用程序认证书对应的应用程序私钥进行签名的值的应用程序质询请求响应信息,利用上述区块链数据库中记录的上述服务器认证书注册事务确认上述应用程序质询请求响应信息,判断上述应用程序认证书是否有效;以及

步骤(d),在上述认证服务器向上述服务提供服务器及上述第二应用程序传递包含上述应用程序认证书是否有效的认证结果消息,从而支援上述服务提供服务器在上述认证结果消息为表示上述应用程序认证书有效的认证成功消息的情况下,向上述第二应用程序传递临时ID(temporary ID),并支援上述第一应用程序能够通过从上述第二应用程序向上述第一应用程序传递的(i)上述临时ID及(ii)上述认证成功消息所包含的访问令牌(access token)利用上述服务,由此对上述登录进行处理。

13.根据权利要求12所述的方法,其特征在于,在进行上述步骤(c)之后,还包括步骤(d0),上述认证服务器将上述认证结果消息或者对此进行加工的值作为认证结果事务记录于上述区块链数据库。

14.根据权利要求12所述的方法,其特征在于,还包括步骤(e),上述认证服务器响应周期性(periodically)或者完整性验证请求,参照上述区块链数据库所记录的(I)服务器认证书的信息或者作为对此进行加工后的值的服务器认证书注册事务,(II)应用程序认证书的信息或者作为对此进行加工后的值的应用程序认证书注册事务,以及(III)认证结果消息或者作为对此进行加工后的值的认证结果事务中的至少一个信息验证上述(I)、(II)、(III)的信息的完整性(integrity)。

15.一种服务提供服务器,用于执行使用区块链数据库通过基于公钥基础设施PKI(public key infrastructure)的认证取代针对利用服务提供服务器所提供的服务的用户的登录请求的登录的方法,其特征在于,包括:

通信部,从用户终端所执行的服务提供应用程序中获得作为通过用户终端所执行的认证应用程序请求取代登录的信息的认证请求信息;以及

处理器,用于执行(i)在作为利用通过基于上述PKI的加密方式生成的服务器公钥和服务器私钥的上述服务提供服务器的认证书的服务器认证书的信息或者作为对此进行加工后的值的服务器认证书注册事务及作为利用通过基于上述PKI的加密方式生成的应用程序公钥和应用程序私钥的认证应用程序的认证书的应用程序认证书的信息或者作为对此进行加工后的值的应用程序认证书注册事务被记录于上述区块链数据库的状态,如果获得上述认证请求信息,则向上述服务提供应用程序传递作为判断是否能够取代上述登录的结果的认证请求响应信息的过程,(ii)从上述认证应用程序获得包含可变认证值的服务器质询请求信息,上述可变认证值为通过上述认证应用程序接收根据来自上述服务提供应用程序的认证重定向请求(authentication redirection request)的质询开始请求信息的认证服务器生成的与上述质询开始请求信息对应的可变认证值,向上述认证应用程序传递与上述服务器质询请求信息相对应的服务器质询请求响应信息,通过上述认证应用程序向上述

认证服务器传递响应请求信息,从而支援上述认证服务器利用上述区块链数据库中记录的上述服务器认证书注册事务和上述应用程序认证书注册事务确认上述响应请求信息,判断上述服务器认证书及上述应用程序认证书是否有效的过程,以及(iii)获得来自上述认证服务器的包含上述服务器认证书及上述应用程序认证书是否有效的认证结果消息,如果上述认证结果消息为表示上述服务器认证书及上述应用程序认证书有效的认证成功消息,则向上述服务提供应用程序传递预定的访问令牌(access token),从而支援上述服务提供应用程序能够通过上述访问令牌利用上述服务,由此对上述登录进行处理的过程。

16.根据权利要求15所述的服务提供服务器,其特征在于,在上述(ii)过程中,上述服务器质询请求信息包含被与上述服务器认证书对应的上述服务器公钥所编码的上述可变认证值,上述处理器利用与上述服务器认证书对应的上述服务器私钥从上述服务器质询请求信息中获得上述可变认证值,并利用上述服务器私钥向上述认证应用程序传递对上述可变认证值进行签名的值的上述服务器质询请求响应信息。

17.一种认证服务器,用于执行使用区块链数据库通过基于公钥基础设施PKI(public key infrastructure)的认证取代针对利用服务提供服务器所提供的服务的用户的登录请求的登录的方法,其特征在于,包括:

通信部,响应与作为通过用户终端所执行的认证应用程序请求取代登录的信息的认证请求信息相对应的认证重定向请求(authentication redirection request),从上述用户终端所执行的认证应用程序中获得质询开始请求信息;以及

处理器,用于执行(i)在作为利用通过基于上述PKI的加密方式生成的服务器公钥和服务器私钥的上述服务提供服务器的认证书的服务器认证书的信息或者作为对此进行加工后的值的服务器认证书注册事务及作为利用通过基于上述PKI的加密方式生成的应用程序公钥和应用程序私钥的认证应用程序的认证书的应用程序认证书的信息或者作为对此进行加工后的值的应用程序认证书注册事务被记录于上述区块链数据库的状态,如果获得上述质询开始请求信息,则生成与上述质询开始请求信息相对应的可变认证值,并向上述认证应用程序传递包含上述可变认证值的质询开始请求响应信息,从而支援上述认证应用程序从上述服务提供服务器获得与用于判断上述服务器认证书是否有效的服务器质询请求信息相对应的服务器质询请求响应信息的过程,(ii)从上述认证应用程序中获得包含利用与上述应用程序认证书对应的应用程序私钥对上述服务器质询请求响应信息进行签名的值的多重签名值的响应请求信息,利用上述区块链数据库中记录的上述服务器认证书注册事务和上述应用程序认证书注册事务确认上述响应请求信息,判断上述服务器认证书及上述应用程序认证书是否有效的过程,以及(iii)向上述认证应用程序及上述服务提供服务器中的至少一个传递包含上述服务器认证书是否有效的认证结果消息,从而在上述认证结果消息为表示上述服务器认证书有效的认证成功消息的情况下,支援上述服务提供服务器向上述用户终端所执行的服务提供应用程序传递预定的访问令牌(access token),由此能够支援上述服务提供应用程序能够通过上述访问令牌利用上述服务,由此对上述登录进行处理的过程。

18.根据权利要求17所述的认证服务器,其特征在于,上述处理器管理与针对上述服务提供服务器的访问级别(accesslevel)相关的信息,或者支援进行管理,并参照上述访问级别决定授权级别(authorizationlevel),上述认证结果消息包含与上述授权级别相关的信

息,而上述服务器认证书是否有效则参照上述授权级别进行判断。

19.根据权利要求17所述的认证服务器,其特征在于,上述处理器利用与上述服务器认证书对应的上述服务器公钥及与上述应用程序认证书对应的上述应用程序公钥对上述多重签名值的签名进行验证,从而判断上述服务器认证书及上述应用程序认证书是否有效。

20.根据权利要求17所述的认证服务器,其特征在于,在上述(ii)过程之后,上述处理器将上述认证结果消息或者对此进行加工的值作为认证结果事务记录于上述区块链数据库。

21.根据权利要求17所述的认证服务器,其特征在于,上述处理器响应周期性(periodically)或者完整性验证请求,参照上述区块链数据库所记录的(I)服务器认证书的信息或者作为对此进行加工后的值的服务器认证书注册事务,(II)应用程序认证书的信息或者作为对此进行加工后的值的应用程序认证书注册事务,以及(III)认证结果消息或者作为对此进行加工后的值的认证结果事务中的至少一个信息验证上述(I)、(II)、(III)的信息的完整性(integrity)。

22.一种服务提供服务器,用于执行使用区块链数据库通过基于公钥基础设施PKI(public key infrastructure)的认证取代针对利用服务提供服务器所提供的服务的用户的登录请求的登录的方法,其特征在于,包括:

通信部,用于从用户终端所执行的第一应用程序中获得包含用户识别信息的认证请求信息,其中,上述用户识别信息用于从接收作为通过上述用户终端所执行的第二应用程序请求取代登录的信息的认证重定向请求(authentication redirection request)的上述第二应用程序中识别上述用户;以及

处理器,用于执行(i)在作为利用通过基于上述PKI的加密方式生成的服务器公钥和服务器私钥的上述服务提供服务器的认证书的服务器认证书的信息或者作为对此进行加工后的值的服务器认证书注册事务及作为利用通过基于上述PKI的加密方式生成的应用程序公钥和应用程序私钥的第二应用程序的认证书的应用程序认证书的信息或者作为对此进行加工后的值的应用程序认证书注册事务被记录于上述区块链数据库的状态,如果获得上述认证请求信息,则向认证服务器传递包含上述用户识别信息的质询开始请求信息的过程,(ii)响应上述质询开始请求信息获得包含通过上述认证服务器生成的可变认证值的质询开始请求响应信息,向上述第二应用程序传递包含上述可变认证值的应用程序质询请求信息,从而支援上述第二应用程序生成利用与上述应用程序认证书对应的上述应用程序私钥对上述可变认证值进行签名的值的过程,(iii)获得包含利用上述应用程序私钥进行签名的值的应用程序质询请求响应信息,向上述认证服务器传递上述应用程序质询请求响应信息,从而支援上述认证服务器利用上述区块链数据库中记录的上述应用程序认证书注册事务确认上述应用程序质询请求响应信息,判断上述应用程序认证书是否有效的过程;以及(iv)从上述认证服务器中获得包含上述应用程序认证书是否有效的认证结果消息,上述认证结果消息为表示上述应用程序认证书有效的认证成功消息,向上述第二应用程序传递临时ID(temporary ID),从而支援上述第一应用程序能够通过从上述第二应用程序向上述第一应用程序传递的上述临时ID及上述认证成功消息所包含的访问令牌(access token)利用上述服务,由此对上述登录进行处理的过程。

23.根据权利要求22所述的服务提供服务器,其特征在于,上述质询开始请求信息还包

含与上述服务器认证书对应的上述服务器公钥,上述质询开始请求响应信息包含通过上述服务器公钥编码的上述可变认证值,其中,在上述(ii)过程中,上述处理器利用与上述服务器认证书对应的上述服务器私钥从上述质询开始请求响应信息中获得上述可变认证值并利用与上述应用程序认证书对应的上述应用程序公钥向上述第二应用程序传递包含对上述可变认证值进行签名的值的上述应用程序质询请求信息。

24.一种认证服务器,用于执行使用区块链数据库通过基于公钥基础设施PKI(public key infrastructure)的认证取代针对利用服务提供服务器所提供的服务的用户的登录请求的登录的方法,其特征在于,包括:

通信部,用于从上述服务提供服务器中获得包含上述用户识别信息的质询开始请求信息,上述服务提供服务器从用户终端所执行的第一应用程序中获得包含用户识别信息的认证请求信息,上述用户识别信息用于从接收作为通过上述用户终端所执行的第二应用程序请求取代登录的信息的认证重定向请求(authentication redirection request)的上述第二应用程序中识别上述用户;以及

处理器,用于执行(i)在作为利用通过基于上述PKI的加密方式生成的服务器公钥和服务器私钥的上述服务提供服务器的认证书的服务器认证书的信息或者作为对此进行加工后的值的服务器认证书注册事务及作为利用通过基于上述PKI的加密方式生成的应用程序公钥和应用程序私钥的上述第二应用程序的认证书的应用程序认证书的信息或者作为对此进行加工后的值的应用程序认证书注册事务被记录于上述区块链数据库的状态,如果获得上述质询开始请求信息,则响应上述质询开始请求信息生成可变认证值的过程,(ii)向上述服务提供服务器传递包含所生成的上述可变认证值的质询开始请求响应信息,从而支援上述服务提供服务器向上述第二应用程序传递包含上述可变认证值的应用程序质询请求信息,由此支援上述第二应用程序生成利用与上述应用程序认证书对应的应用程序私钥对上述可变认证值进行签名的值的过程,(iii)获得包含利用与上述应用程序认证书对应的应用程序私钥进行签名的值的应用程序质询请求响应信息,利用上述区块链数据库中记录的上述应用程序认证书注册事务确认上述应用程序质询请求响应信息,判断上述应用程序认证书是否有效的过程,以及(iv)向上述服务提供服务器及上述第二应用程序传递包含上述应用程序认证书是否有效的认证结果消息,从而支援上述服务提供服务器在上述认证结果消息为表示上述应用程序认证书有效的认证成功消息的情况下,向上述第二应用程序传递临时ID(temporary ID),并支援上述第一应用程序能够通过从上述第二应用程序向上述第一应用程序传递的上述临时ID及上述认证成功消息所包含的访问令牌(access token)利用上述服务,由此对上述登录进行处理的过程。

25.根据权利要求24所述的认证服务器,其特征在于,在上述(iii)过程之后,上述处理器将上述认证结果消息或者对此进行加工的值作为认证结果事务记录于上述区块链数据库。

26.根据权利要求24所述的认证服务器,其特征在于,上述处理器响应周期性(periodically)或者完整性验证请求,参照上述区块链数据库所记录的(I)服务器认证书的信息或者作为对此进行加工后的值的服务器认证书注册事务,(II)应用程序认证书的信息或者作为对此进行加工后的值的应用程序认证书注册事务,以及(III)认证结果消息或者作为对此进行加工后的值的认证结果事务中的至少一个信息验证上述(I)、(II)、(III)

的信息的完整性(integrity)。

使用基于UTXO的协议的区块链数据库并通过基于PKI的认证取代用户的登录的方法及利用其的服务器

技术领域

[0001] 本发明涉及使用基于UTXO(unspent transaction output)协议的区块链数据库通过基于公钥基础设施(public key infrastructure,PKI)的认证取代针对利用服务提供服务器所提供的服务的用户的登录请求的登录的方法、对此进行执行的服务提供服务器及认证服务器。

背景技术

[0002] 以往作为用于取代用户个人账户的登录的服务,OAuth2.0为在网络、手机及桌面应用程序等中实现标准化的认证方式,是利用可以安全地进行认证的开放型协议的方式。在利用这种OAuth之前,由于没有认证方式的标准,因而利用了以往作为基本认证的用户名和密码的组合,而这在安保方面是脆弱的。在并非为基本认证的情况下,各应用程序分别按所开发的公司的方法确认了用户,而这些方法中包括了谷歌的AuthSub、AOL的OpenAuth、雅虎的BBAuth、亚马逊的网络服务API等。OAuth作为像这样对各自的认证方式进行标准化的认证方式,如果利用OAuth,对上述认证进行共享的应用程序之间就不需要额外的认证。因此,可以合并多种应用程序使用,而OAuth2.0为这种OAuth的最新版本。如果对这种OAuth2.0的方式进行简要说明如下。

[0003] 当用户想要利用由服务提供服务器所提供的服务时,首先根据用户的操作,从作为上述用户的终端的用户终端向上述服务提供服务器传递用于登录的认证请求。

[0004] 接收认证请求的服务提供服务器向认证服务器传输登录信息,认证服务器对上述登录信息进行验证,由此,如果成功结束验证,则向服务提供服务器返还授权信息。

[0005] 根据上述授权信息,服务提供服务器向用户终端传输预定的授权传递信息,而接收这种授权传递信息的用户终端向认证服务器传递用于请求访问令牌(access token)的信息,从而获得通过认证服务器发放的访问令牌。那样的话,用户终端可以持有上述访问令牌向服务提供服务器请求与服务相关的资源,从而结束登录取代程序。

[0006] 另一方面,服务提供服务器可以为了确认从用户终端中获得的访问令牌是否有效而向认证服务器请求针对访问令牌的验证请求,而响应于此,认证服务器可以返还用户的多个属性信息。

[0007] 由于这种以往的OAuth也因其认证程序仅通过确认用户ID(用户识别信息)及密码是否一致实现,因此,当用户ID及密码被盗时,仍然存在安保脆弱的问题。可以为了提高安全性而导入的认证书,例如,以往的公认认证书大致需要高额的发放费用,并且伴随着使用方面的制约,因此,优选地,利用安全性和使用性强且重新替代以往的公认认证书等的基于区块链的认证书。

[0008] 为此,本发明人提出并不局限于现有的OAuth2.0的协议而利用基于区块链的技术,从而在安全性方面比以往的OAuth2.0协议更加强化,并且可以取代多种结构的个人或者服务器等的认证的方法。

发明内容

[0009] 技术问题

[0010] 本发明提供用于强化上述的现有OAuth的安全性和使用性的方法及服务器，本发明的目的在于，提供安全性和使用性强，且能够以低廉的费用替代以往的方式的技术方案。

[0011] 具体地，本发明的目的在于，提供参照被记录于虚拟货币的私人/公共区块链数据库的认证书相关信息，并在这样的区块链数据库记录与认证结果相关的信息，从而最终无法实现伪造变造的方案。

[0012] 而且，本发明的目的在于，并非利用多重签名只对用户个人的认证书进行验证，而是对成为服务请求对象的服务提供服务器的认证书也一同进行验证，从而提高安全性。

[0013] 另一方面，本发明的目的在于，因可以提供临时ID而对不具有用户ID的用户也可以提供服务，并强化安保。

[0014] 并且，本发明的另一目的在于，以如上所述的方式利用被记录于区块链数据库的事务执行针对相关信息的验证，从而可以保证数据库的完整性(integrity)。

[0015] 本发明的又一目的在于，提供具有可以针对多种结构的个人或者服务器取代认证的机构的基于区块链的登录取代服务提供体系。

[0016] 解决问题的方法

[0017] 用于实现如上所述的本发明的目的，并实现后述的本发明的特征性效果的本发明的特征性构成如下。

[0018] 根据本发明的一实施方式，提供使用区块链数据库通过基于公钥基础设施(public key infrastructure,PKI)的认证取代针对利用服务提供服务器所提供的服务的用户的登录请求的登录的方法，上述方法包括：步骤(a)，如果从上述用户终端所执行的服务提供应用程序中获得作为请求通过用户终端所执行的认证应用程序取代登录的信息的认证请求信息，则上述服务提供服务器向上述服务提供应用程序传递作为判断是否能够取代上述登录的结果的认证请求响应信息；步骤(b)，如果在向上述认证应用程序传递上述服务提供应用程序的认证重定向请求(authentication redirection request)后，从上述认证应用程序获得包含认证服务器生成的可变认证值的服务器质询请求信息，则上述服务提供服务器向上述认证应用程序传递与上述服务器质询请求信息相对应的服务器质询请求响应信息，从而支援上述认证服务器判断作为上述服务提供服务器的认证书的服务器认证书及作为上述认证应用程序的认证书的应用程序认证书是否有效的步骤；以及步骤(c)，从上述认证服务器获得包含上述服务器认证书及上述应用程序认证书是否有效的认证结果消息，如果上述认证结果消息为表示上述服务器认证书及上述应用程序认证书有效的认证成功消息，则上述服务提供服务器向上述服务提供应用程序传递预定的访问令牌(access token)，从而支援上述服务提供应用程序能够通过上述访问令牌利用上述服务，由此对上述登录进行处理。

[0019] 根据本发明的另一实施方式，提供使用区块链数据库通过基于公钥基础设施(public key infrastructure,PKI)的认证取代针对利用服务提供服务器所提供的服务的用户的登录请求的登录的方法，上述方法包括：步骤(a)，如果响应与作为请求通过用户终端所执行的认证应用程序取代登录的认证请求信息相对应的认证重定向请求(authentication redirection request)，从通过上述用户终端执行的认证应用程序中获

得质询开始请求信息，则认证服务器生成与上述质询开始请求信息相对应的可变认证值，向上述认证应用程序传递包含上述可变认证值的质询开始请求响应信息，从而使上述认证应用程序从上述服务提供服务器获得服务器质询请求响应信息，上述服务器质询请求响应信息与用于判断作为上述服务提供服务器的认证书的服务器认证书是否有效的服务器质询请求信息相对应；步骤(b)，如果利用作为上述认证应用程序的认证书的应用程序认证书的私钥(private key)从上述认证应用程序中获得包含作为对上述服务器质询请求响应信息进行签名的值的多重签名值的响应请求信息，则上述认证服务器利用上述响应请求信息判断上述服务器认证书及上述应用程序认证书是否有效；以及步骤(c)，上述认证服务器向上述认证应用程序及上述服务提供服务器中的至少一个传递包含上述服务器认证书是否有效的认证结果消息，从而在上述认证结果消息为表示上述服务器认证书有效的认证成功消息的情况下，支援上述服务提供服务器向通过上述用户终端执行的服务提供应用程序传递预定的访问令牌(access token)，由此支援上述服务提供应用程序能够通过上述访问令牌利用上述服务，由此对上述登录进行处理。

[0020] 根据本发明的又一实施方式，提供使用区块链数据库通过基于公钥基础设施(public key infrastructure,PKI)的认证取代针对利用服务提供服务器所提供的服务的用户的登录请求的登录的方法，上述方法包括：步骤(a)，如果从用户终端所执行的第一应用程序中获得包含用于从接收作为通过上述用户终端所执行的第二应用程序请求取代登录的信息的认证重定向请求(authentication redirection request)的上述第二应用程序中识别上述用户的用户识别信息的认证请求信息，则上述服务提供服务器向认证服务器传递包含上述用户识别信息的质询开始请求信息；步骤(b)，如果响应上述质询开始请求信息获得包含由上述认证服务器生成的可变认证值的质询开始请求响应信息，则上述服务提供服务器向上述第二应用程序传递包含上述可变认证值的应用程序质询请求信息，从而支援上述第二应用程序生成利用作为上述第二应用程序的认证书的应用程序认证书的私钥(private key)对上述可变认证值进行签名的值；步骤(c)，如果获得包含利用上述应用程序认证书的私钥(private key)进行签名的值的应用程序质询请求响应信息，则上述服务提供服务器向上述认证服务器传递上述应用程序质询请求响应信息，从而支援上述认证服务器利用上述应用程序质询请求响应信息判断上述应用程序认证书是否有效；以及步骤(d)，如果从上述认证服务器中获得包含上述应用程序认证书是否有效的认证结果消息，并且上述认证结果消息为表示上述应用程序认证书有效的认证成功消息，则上述服务提供服务器向上述第二应用程序传递临时ID(temporary ID)，并支援上述第一应用程序能够通过从上述第二应用程序向上述第一应用程序传递的(i)上述临时ID及(ii)上述认证成功消息所包含的访问令牌(access token)利用上述服务，由此对上述登录进行处理。

[0021] 再次，根据本发明的一实施方式，提供使用区块链数据库通过基于公钥基础设施(public key infrastructure,PKI)的认证取代针对利用服务提供服务器所提供的服务的针对用户的登录请求的登录的方法，上述方法包括：步骤(a)，如果从上述服务提供服务器获得包含上述用户识别信息的质询开始请求信息，其中，上述服务提供服务器从用户终端所执行的第一应用程序中获得包含用于从接收作为通过上述用户终端所执行的第二应用程序请求取代登录的信息的认证重定向请求(authentication redirection request)的上述第二应用程序中识别上述用户的用户识别信息的认证请求信息，则认证服务器响应上

述质询开始请求信息生成可变认证值;步骤(b),向上述服务提供服务器传递包含所生成的上述可变认证值的质询开始请求响应信息,从而支援上述服务提供服务器向上述第二应用程序传递包含上述可变认证值的应用程序质询请求信息,由此支援上述第二应用程序生成利用作为上述第二应用程序的认证书的应用程序认证书的私钥(private key)对上述可变认证值进行签名的值;步骤(c),如果获得包含利用上述应用程序认证书的私钥(private key)进行签名的值的应用程序质询请求响应信息,则上述认证服务器利用上述应用程序质询请求响应信息判断上述应用程序认证书是否有效;以及步骤(d),在上述认证服务器向上述服务提供服务器及上述第二应用程序传递包含上述应用程序认证书是否有效的认证结果消息,从而支援上述服务提供服务器在上述认证结果消息为表示上述应用程序认证书有效的认证成功消息的情况下,向上述第二应用程序传递临时ID(temporary ID),并支援上述第一应用程序能够通过从上述第二应用程序向上述第一应用程序传递的(i)上述临时ID及(ii)上述认证成功消息所包含的访问令牌(access token)利用上述服务,从而对上述登录进行处理。

[0022] 根据本发明的另一实施方式,提供上述服务提供服务器,用于执行使用区块链数据库通过基于公钥基础设施(public key infrastructure,PKI)的认证取代针对利用服务提供服务器所提供的服务的针对用户的登录请求的登录的方法,上述服务器包括:通信部,从用户终端所执行的服务提供应用程序中获得作为通过用户终端所执行的认证应用程序请求取代登录的认证请求信息;以及处理器,用于执行(i)如果获得上述认证请求信息,则向上述服务提供应用程序传递作为判断是否能够取代上述登录的结果的认证请求响应信息的过程,(ii)如果在向上述认证应用程序传递上述服务提供应用程序的认证重定向请求(authentication redirection request)之后,获得包含从上述认证应用程序中通过认证服务器生成的可变认证值的服务器质询请求信息,则向上述认证应用程序传递与上述服务器质询请求信息相对应的服务器质询请求响应信息,从而支援上述认证服务器判断作为上述服务提供服务器的认证书的服务器认证书及作为上述认证应用程序的认证书的应用程序认证书是否有效的过程,以及(iii)从上述认证服务器获得包含上述服务器认证书及上述应用程序认证书是否有效的认证结果消息,如果上述认证结果消息为表示上述服务器认证书及上述应用程序认证书有效的认证成功消息,则向上述服务提供应用程序传递预定的访问令牌(access token),从而支援上述服务提供应用程序能够通过上述访问令牌利用上述服务,由此对上述登录进行处理的过程。

[0023] 根据本发明的又一实施方式,提供认证服务器,用于执行使用区块链数据库利用服务提供服务器所提供的服务的针对用户的登录请求进行通过基于公钥基础设施(public key infrastructure,PKI)的认证取代登录的方法,上述服务器包括:通信部,响应与作为请求取代通过用户终端所执行的认证应用程序的登录的认证请求信息相对应的认证重定向请求(authentication redirection request),从上述用户终端所执行的认证应用程序中获得质询开始请求信息,或者支援其他装置获得;以及处理器,用于执行(i)如果获得上述质询开始请求信息,则生成与上述质询开始请求信息相对应的可变认证值,并向上述认证应用程序传递包含上述可变认证值的质询开始请求响应信息,或者支援其他装置进行传递,从而支援上述认证应用程序从上述服务提供服务器获得与用于判断作为上述服务提供服务器的认证书的服务器认证书是否有效的服务器质询请求信息相对应的服务器质询请

求响应信息的过程,(ii)如果从上述认证应用程序中获得包含利用作为上述认证应用程序的认证书的应用程序认证书的私钥(private key)对上述服务器质询请求响应信息进行签名的值的多重签名值的响应请求信息,则利用上述响应请求信息判断上述服务器认证书及上述应用程序认证书是否有效的过程,以及(iii)向上述认证应用程序及上述服务提供服务器中的至少一个传递包含上述服务器认证书是否有效的认证结果消息,从而在上述认证结果消息为表示上述服务器认证书有效的认证成功消息的情况下,支援上述服务提供服务器向上述用户终端所执行的服务提供应用程序传递预定的访问令牌(access token),由此能够支援上述服务提供应用程序能够通过上述访问令牌利用上述服务,由此对上述登录进行处理的过程。

[0024] 根据本发明的又一实施方式,提供上述服务提供服务器,用于执行使用区块链数据库通过基于公钥基础设施(public key infrastructure,PKI)的认证取代针对利用服务提供服务器所提供的服务的用户的登录请求的登录的方法,上述服务器包括:通信部,用于从用户终端所执行的第一应用程序中获得包含用户识别信息的认证请求信息,其中,上述用户识别信息用于从接收作为通过上述用户终端所执行的第二应用程序请求取代登录的信息的认证重定向请求(authentication redirection request)的上述第二应用程序中识别上述用户;以及处理器,用于执行(i)如果获得上述认证请求信息,则向认证服务器传递包含上述用户识别信息的质询开始请求信息的过程,(ii)如果响应上述质询开始请求信息获得包含通过上述认证服务器生成的可变认证值的质询开始请求响应信息,则上述服务提供服务器向上述第二应用程序传递包含上述可变认证值的应用程序质询请求信息,从而支援上述第二应用程序生成利用作为上述第二应用程序的认证书的应用程序认证书的私钥(private key)对上述可变认证值进行签名的值的过程,(iii)如果获得包含利用上述应用程序认证书的私钥(private key)进行签名的值的应用程序质询请求响应信息,则向上述认证服务器传递上述应用程序质询请求响应信息,从而支援上述认证服务器利用上述应用程序质询请求响应信息判断上述应用程序认证书是否有效的过程;以及(iv)如果从上述认证服务器中获得包含上述应用程序认证书是否有效的认证结果消息,并且上述认证结果消息为表示上述应用程序认证书有效的认证成功消息,则向上述第二应用程序传递临时ID(temporary ID),从而支援上述第一应用程序能够通过从上述第二应用程序向上述第一应用程序传递的上述临时ID及上述认证成功消息所包含的访问令牌(access token)利用上述服务,由此对上述登录进行处理的过程。

[0025] 根据本发明的又一实施方式,提供认证服务器,用于执行使用区块链数据库通过基于公钥基础设施(public key infrastructure,PKI)的认证取代针对利用服务提供服务器所提供的服务的针对用户的登录请求的登录的方法,上述服务器包括:通信部,用于从上述服务提供服务器中获得包含上述用户识别信息的质询开始请求信息,上述服务提供服务器从用户终端所执行的第一应用程序中获得包含用户识别信息的认证请求信息,上述用户识别信息用于从接收作为通过上述用户终端所执行的第二应用程序请求取代登录的信息的认证重定向请求(authentication redirection request)的上述第二应用程序中识别上述用户;以及处理器,用于执行(i)如果获得上述质询开始请求信息,则响应上述质询开始请求信息生成可变认证值的过程,(ii)向上述服务提供服务器传递包含所生成的上述可变认证值的质询开始请求响应信息,从而支援上述服务提供服务器向上述第二应用程序传

递包含上述可变认证值的应用程序质询请求信息,由此支援上述第二应用程序生成利用作为上述第二应用程序的认证书的应用程序认证书的私钥(private key)对上述可变认证值进行签名的值的过程,(iii)如果获得利用上述应用程序认证书的私钥(private key)进行签名的值的应用程序质询请求响应信息,则利用上述应用程序质询请求响应信息判断上述应用程序认证书是否有效的过程,以及(iv)向上述服务提供服务器及上述第二应用程序传递包含上述应用程序认证书是否有效的认证结果消息,从而支援上述服务提供服务器在上述认证结果消息为表示上述应用程序认证书有效的认证成功消息的情况下,向上述第二应用程序传递临时ID(temporary ID),并支援上述第一应用程序能够通过从上述第二应用程序向上述第一应用程序传递的上述临时ID及上述认证成功消息所包含的访问令牌(access token)利用上述服务,由此对上述登录进行处理的过程。

[0026] 发明的效果

[0027] 根据本发明的方法,具有安全性和使用性强,且能够以低廉的费用替代以往的OAuth的效果。

[0028] 并且,根据本发明的方法,具有提供通过高级别的加密、多重签名、交叉验证的临时ID的发放等的高的安保级别。

[0029] 并且,根据本发明的方法,具有在根本上防止认证书相关信息的伪造变造,从而保证可靠性的效果。

附图说明

[0030] 以下用于说明本发明的实施例的附图仅为本发明的多个实施例中的一部分,对于本发明所属技术领域的普通技术人员(以下称之为“普通技术人员”)而言,可以在不进行发明作业的情况下,基于这些附图获得其他附图。

[0031] 图1为简要示出根据第一实施例至第三实施例执行取代登录的方法的服务提供服务器、认证服务器及用户终端的例示性构成的概念图;

[0032] 图2为以例示性的方式示出根据本发明的第一实施例至第三实施例,通过利用服务器认证书和应用程序认证书的多重签名取代登录的方法的序列图(sequence diagram);

[0033] 图3为以例示性的方式示出根据本发明的第一实施例至第三实施例,在没有用户ID的状态下,利用多重信息取代登录的方法的序列图;

[0034] 图4及图5为简要示出根据本发明的第二实施例,多个事务被记录于预定的数据库的过程的概念图;

[0035] 图6及图7为以例示性的方式示出根据本发明的第三实施例,将各个认证书的使用次数限制在initNumber和10次的智能合约(源代码)的示意图。

具体实施方式

[0036] 后述的针对本发明的详细说明将参照为了使本发明的多个目的、多个技术方案及多个优点更加明确而将由能够实施本发明的特定实施例作为例示图示的附图。这些实施例将进行详细说明,以便让普通技术人员能够足以实施本发明。

[0037] 在本说明书中,“数据库”意味着体系化的数据,即,得到合并管理的信息的集合及对此进行管理的系统,包含普通关系型数据库、蒙戈数据库(MongoDB)及区块链数据库中的

至少一部分，但并不局限于此。普通技术人员可以理解，虽然在本说明书中为了便于说明而对虚拟货币的区块链数据库进行说明，但也可以在其他种类的数据库中实现变形实施。

[0038] 在本说明书中，“公共区块链数据库”是指，使用掌管作为虚拟货币的区块链广泛用于公共的区块链即公共区块链的虚拟货币系统上的所有计算装置作为数据库的技术。

[0039] 并且，在本说明书中，“私人区块链数据库”是指，利用虚拟货币的区块链，但并非利用上述用于公共的公共区块链，而是利用根据本发明的认证服务器直接管理的所谓单独构成的私人区块链的数据库。

[0040] 上述虚拟货币是指通过以适用区块链技术的电子钱包为基础的事务(transaction)流通的数字货币，虚拟货币有比特币、莱特币、暗黑币、域名币、多吉币及瑞波币等。

[0041] 而且，在本说明书中，“智能合约”为通过可执行的字节码编译，从而能够在至少一个计算装置上得到执行的代码，并且，当进行上述执行时，只要满足特定条件，就执行预先指定的程序，而作为上述执行的结果的执行结果值的完整性是指，以通过对上述至少一个计算装置所计算出的上述执行结果值的一致性(consensus)得到验证为特征的概念。

[0042] 并且，在本发明的详细说明及多个权利要求中，术语“包含”及其变形并非用于排除其他多个技术特征、附加物、构成要素或者步骤。对于普通技术人员而言，本发明的多个其他目的、优点及特性的一部分将从本说明书中展现出，而且，一部分将从本发明的实施中展现出。以下的例示及附图将作为实例提供，而非用于限制本发明。

[0043] 而且，本发明包括本说明书所表示的多个实施例的所有可能的组合。应该理解的是，本发明的多种实施例虽然互不相同，但并不需要相互排斥。例如，在此所记载的特定形状、结构及特性可以一边与一实施例相关地不脱离本发明的精神及范围，一边以其他实施例体现。并且，应该理解的是，各个公开的实施例内的个别的构成要素的位置或者配置可以在不脱离本发明的精神及范围的情况下得到变更。因此，后述的详细说明并不作为限定的含义采用，本发明的范围只要得到适当的说明，就与其多个权利要求所主张的内容等同的所有范围一同被所附权利要求所限定。在附图中，类似的附图标记在多个侧面指相同或类似的功能。

[0044] 本发明的第一实施例为以利用虚拟货币的UTXO(unspent transaction output)，将有关其UTXO的个别事务记录于预定的区块链数据库的方式构成的实施例。

[0045] 本发明的第二实施例为以利用虚拟货币的UTXO，将有关其UTXO的个别事务记录于第一区块链数据库之后，在第二区块链数据库中记录从被记录于上述第一区块链数据库的多个事务中生成的代表哈希值，从而双重谋求记录的完整性的锚定(anchoring)方式构成的实施例。

[0046] 本发明的第三实施例为以利用用于管理因智能合约而有所不同的认证书相关的状态(state)的信息的状态数据库(SDB;state database)，并且在预定的区块链数据库记录事务，在状态数据库中记录状态的变更事项的方式构成的实施例。

[0047] 作为参考，在本发明中，如果上述第一区块链数据库为直接记录数据的区块链数据库，则上述第二区块链数据库可以被视为为了数据的完整性而经由上述第一区块链数据库间接地得到记录的区块链数据库。

[0048] 在本说明书中，以不同的方式表示或者在上下文中明确地不矛盾的情况下，以单

数表示的项目只要在其上下文中没有另行要求，就包括复数的表示。以下，为了让普通技术人员容易地实施本发明，参照附图对本发明的优选的实施例进行详细说明。

[0049] 图1为简要示出根据执行取代登录的方法的服务提供服务器、认证服务器及用户终端的例示性构成的概念图。

[0050] 参照图1，本发明一实施例的认证服务器、服务提供服务器及用户终端作为典型的计算装置100(例如，可以包括计算机处理器、存储器、存储装置、输入装置及输出装置、其他以往的计算装置的多个构成要素的装置；路由器、开关之类的电子通信装置；网络附属存储(NAS)及存储区域网络(SAN)之类的电子信息存储系统)，可以利用计算机软件(即，使计算装置以特定的方式实现功能的多个指令)的组合执行本发明的方法，这种计算装置100包括通信部110、处理器120，并且，能够相互以间接或者直接的方式进行通信。

[0051] 这种计算装置的通信部110可以与联动的其他计算装置收发请求和响应，作为一例示，这种请求和响应可以通过相同的TCP会话实现，但本发明并不局限于此，例如，还能够以UDP数据报的方式进行收发。

[0052] 并且，计算装置的处理器120可以包括MPU(Micro Processing Unit)或者CPU(Central Processing Unit)、高速缓冲存储器(Cache Memory)、数据总线(Data Bus)等硬件结构。并且，还可以包括操作系统、用于执行特定目的的应用程序的软件构成。

[0053] 第一实施例

[0054] 以下从第一实施例开始说明根据本发明取代登录的方法。

[0055] 图2为以例示性的方式表示根据本发明，通过利用服务器认证书和应用程序认证书的多重签名取代登录的方法(以下称之为“多重签名登录取代方法”)的序列图(sequence diagram)。

[0056] 参照图2，本发明第一实施例的多重签名登录取代方法包括：如果从用户终端所执行的服务提供应用程序中获得作为通过用户所利用的上述用户终端所执行的认证应用程序请求取代登录的信息的认证请求信息(步骤S210)，则上述服务提供服务器向上述服务提供应用程序传递作为判断是否能够取代上述登录的结果的认证请求响应信息(步骤S215)的步骤S210、步骤S215。

[0057] 其中，上述认证请求信息可以包含作为用于定义认证的类型的信息的认证类型(auth type)信息。例如，上述认证类型信息相当于根据在用户想要使用服务时是仅仅利用简单的查询等服务还是利用结算等重要的服务等服务的轻重，使得能够进行选择请求的认证的种类的参数。

[0058] 并且，上述认证请求信息可以包含能够识别上述认证应用程序的认证应用程序识别信息，而获得上述认证应用程序识别信息的服务提供服务器能够基于(i)上述服务提供服务器所提供的服务是否允许通过上述认证应用程序取代登录，(ii)如果上述服务允许通过上述认证应用程序取代登录，则基于上述登录的取代是否允许上述用户等信息判断是否可以取代上述登录，而其结果可以作为认证请求响应信息进行返还。

[0059] 例如，为了判断是否允许对上述用户的登录的取代，上述认证请求信息还可以包含用于识别上述用户终端的信息及用于识别上述服务提供应用程序的信息中的至少一个，但并不局限于从，普通技术人员可以提出允许上述服务提供服务器通过上述认证应用程序取代登录的多种基准。

[0060] 上述认证请求响应信息可以包含上述认证应用程序识别信息、授权级别(authorization level)、能够识别服务提供服务器的服务提供服务器识别信息及推荐人服务密钥(referrer service key)中的至少一个信息。

[0061] 其中,授权级别是指用户利用本发明的登录取代,从而从服务提供服务器中获得的服务的级别、范围及程度,上述授权级别为每次进行登录取代时由认证服务器所提供的值,并且,被指定为等于或小于作为通过认证服务器对相应的服务提供服务器实施固有设置的值的访问级别(access level)的级别。访问级别是在注册作为服务提供服务器的认证书的服务器认证书时,由认证服务器所指定,对此将进行详细后述。

[0062] 并且,其中,推荐人服务密钥(referrer service key)作为在用户利用本发明的取代登录的方法的过程中,为了识别执行上述方法的会话(session)的相同性而利用的值,是由上述服务提供服务器所提供的值。

[0063] 另一方面,在第一实施例中,上述步骤S210、步骤S215的特征在于,可以在作为上述服务提供服务器的认证书的服务器认证书的信息或者作为对此进行加工后的值的服务器认证书注册事务及作为上述认证应用程序的认证书的应用程序认证书的信息或者作为对此进行加工的值的应用程序认证书注册事务被记录于上述区块链数据库的状态执行。其中,上述区块链数据库可以为私人区块链数据库或者公共区块链数据库。

[0064] 在本说明书中,认证书,即,上述服务器认证书及上述应用程序认证书通常意味着利用通过基于上述公钥基础设施(public key infrastructure,PKI)的加密方式生成的公钥(public key)及私钥(private key)的认证书。

[0065] 可以在用于注册上述认证书的认证书的注册阶段向认证服务器传递的认证书的信息可以包含例如,(i)通过基于上述公钥基础设施(public key infrastructure,PKI)的加密方式生成的公钥(public key)PubA。上述认证书的信息还可以包含(ii)作为对用于识别上述认证书的利用主体的识别信息进行哈希计算的结果值的识别信息哈希值IdhashA,上述认证书的信息(iii)作为用于对基于上述PKI的加密方式的种类及上述哈希计算的种类中的至少一个进行特定的信息,还可以包含加密类型(crypto type)、(iv)许可证密钥(license key)、(v)许可证级别(license level)之类的追加信息中的至少一个。

[0066] 具体地,许可证密钥为服务提供服务器的运营人员和认证服务器的运营人员之间预先协商好的预定的信息。因此,在上述许可证密钥与预先协商的密钥不同,或者许可证密钥的形态不按照所指定的规格的情况下,也可以判断向认证服务器传递的信息为用于入侵的流量。另一方面,对于认证服务器的运营人员而言,如果结束与服务提供服务器的运营人员之间的契约关系,则可以将相应的许可证密钥变更为无法利用的状态。

[0067] 并且,许可证级别相当于为了取代登录而通过认证服务器向服务提供服务器提供的服务的级别、范围及程度,而上述许可证级别可以为通过上述协商预先指定的值。

[0068] 另一方面,上述认证书的信息作为针对通过上述认证服务器获得的上述(i)至(v)的信息的响应,还可以包含在认证书的注册阶段生成的信息,而这可以是能够识别上述认证书的认证书识别信息及访问级别(access level)中的至少一个信息。在上述认证书为服务器认证书的情况下,上述认证书识别信息为服务器认证书识别信息,在上述认证书为应用程序认证书的情况下,上述认证书识别信息为应用程序认证书识别信息。

[0069] 上述访问级别意味着在通过上述认证书接受上述登录取代服务时,可以通过上述

认证书进行访问的服务的范围和程度，虽然上述许可证级别为认证服务器和服务提供服务器之间的固有的值，但相反，上述访问级别作为在发放服务器认证书时通过认证服务器向服务提供服务器赋予的，是认证书固有的值。访问级别可以通过认证服务器指定为等于或小于许可证级别。

[0070] 并且，上述识别信息哈希值IdhashA可以为针对上述利用主体，例如，作为服务提供服务器的利用主体的服务供应商、用户终端所利用的认证应用程序或者作为第二应用程序的利用主体的用户等的识别信息的法人或者个人的信息进行哈希计算的结果值。普通技术人员可以理解，上述识别信息可以包含例如名称(姓名)、设立年月日(出生年月日)、联系方式信息、电子邮件中的至少一个，但并不局限于此。

[0071] 并且，用于上述哈希计算的哈希函数可以包含MD4函数、MD5函数、SHA-0函数、SHA-1函数、SHA-224函数、SHA-256函数、SHA-384函数、SHA-512函数及HAS-160函数。但并不局限于此。例如，也可以是Triple SHA256。

[0072] 另一方面，参照被记录于上述区块链数据库的上述服务器认证书注册事务及上述应用程序认证书注册事务，从而可以验证上述服务器认证书及上述应用程序认证书的完整性。对此，将进行详细后述。

[0073] 然后，本发明的第一实施例的多重签名登录取代方法还包括步骤S220至步骤S250，即，如果在向上述认证应用程序传递上述服务提供应用程序的认证重定向请求(authentication redirection request)(步骤S220)之后，获得包含从上述认证应用程序中通过认证服务器生成的可变认证值的服务器质询请求信息(步骤S230、步骤S235)，则上述服务提供服务器向上述认证应用程序传递与上述服务器质询请求信息相对应的服务器质询请求响应信息(步骤S240)，从而支援上述认证服务器判断作为上述服务提供服务器的认证书的服务器认证书及作为上述认证应用程序的认证书的应用程序认证书是否有效(步骤S245至步骤S250)

[0074] 其中，认证重定向请求可以包含能够识别服务提供应用程序的服务提供应用程序识别信息、用于识别所提供的服务的类型的服务类型(service type)信息、上述认证级别、能够识别服务提供服务器的服务提供服务器识别信息及推荐人服务密钥中的至少一个。

[0075] 并且，其中，可变认证值作为用于验证上述服务器认证书及上述应用程序认证书是否有效的值，属于一次性编号，例如，可以为时间戳值(timestamp)，但并不局限于此。例如，可以为从任意的种子(seed)值生成的预定的随机数值(random nonce)，即，随机值(random value)。像这样生成可变认证值的方法在理解本发明方面属于不必要的细节，因此，将不再进行详细说明，而这与普通技术人员公知或容易理解的内容相同。

[0076] 而且，其中，服务器质询请求信息还可以包含推荐人认证密钥(referrer auth key)及上述推荐人服务密钥中的至少一个信息。推荐人认证密钥作为在用户利用本发明的登录取代方法的过程中，为了识别是通过哪个认证应用程序，哪个服务提供服务器进行传递的质询开始请求，即，为了识别认证应用程序及服务提供服务器而利用的值，是通过上述认证服务器提供的值。上述推荐人认证密钥作为被包含于从上述认证服务器向认证应用程序传递的质询开始请求响应信息的值，针对上述质询开始请求响应信息将进行后述。

[0077] 另一方面，与服务器质询请求信息相对应的服务器质询请求响应信息还可以包含上述推荐人认证密钥、服务类型信息、授权级别及服务提供服务器识别信息中的至少一个。

[0078] 在本发明所利用的基于PKI的加密方式中，就执行上述方法的多个主体之间进行收发的信息而言，发送的一方所要发送的信息通常利用公钥(public key)进行编码(encoding)。接收的一方可以利用接收上述被编码的信息的一方的私钥(private key)进行解码(decoding)，从而可以获得所要发送的信息。在这种情况下，具体地，上述服务器质询请求信息可以包含被上述服务器认证书的公钥(public key)所编码的上述可变认证值。那样的话，上述服务提供服务器可以利用上述服务器认证书的私钥从上述服务器质询请求信息中获得上述可变认证值，并可以利用上述服务器认证书的私钥向上述认证应用程序传递包含有对上述可变认证值进行签名的值的上述服务器质询请求响应信息。只不过，想要发送的信息有可能并非为利用接收的一方的公钥(public key)进行编码(encoding)的。假设也有可能利用普遍公知的对称密钥加密方式(symmetric-key algorithm)。

[0079] 在进行上述步骤S220至步骤S250之后，本发明的第一实施例的多重签名登录取代方法还包括步骤S260a、步骤S260b及步骤S270，即，从上述认证服务器获得包含上述服务器认证书及上述应用程序认证书是否有效的认证结果消息(S260a，S260b)，如果上述认证结果消息为表示上述服务器认证书及上述应用程序认证书有效的认证成功消息，则上述服务提供服务器向上述服务提供应用程序传递预定的访问令牌(access token)(步骤S270)，从而支援上述服务提供应用程序可以通过上述访问令牌使用上述服务，由此，对上述登录进行处理。

[0080] 其中，上述认证结果消息还可以包含上述应用程序认证书识别信息，并且，还可以包含上述服务提供应用程序识别信息及服务提供服务器识别信息中的至少一个。

[0081] 并且，上述访问令牌作为为了利用上述服务而由执行上述服务提供应用程序的用户终端向上述服务提供服务器传递的预定的信息，可以为美国信息交换标准代码(ASCII)值或者二进制(binary)值。上述访问令牌为用于识别利用上述服务提供应用程序的用户的唯一值(unique value)，并且，应以防止泄漏的方式进场存储。因此，也可以根据基于PKI的加密方式进行传递。上述访问令牌可以为所发放的主体设定预定的有效期间并在以后过有效期间的情况下被无效化的值。

[0082] 作为一例示，上述访问令牌可以为在OAuth认证方式中所提供的访问令牌，而在这种情况下，上述访问令牌可以为字母数字和特殊文字的组合。例如，在OAuth认证方式中所提供的访问令牌可以为如“fb2e77d.47a0479900504cb3ab4a1f626d174d2d”之类的形态，而普通技术人员可以很好地理解作为一例示所提供的OAuth认证方式所利用的访问令牌。

[0083] 如果以认证服务器为基准重新说明上述的本发明第一实施例的多重签名登录取代方法如下，多重签名登录取代方法包括步骤S210至步骤S245，即，首先，如果响应与作为通过用户终端所执行的认证应用程序请求取代登录的信息的认证请求信息(步骤S210)相对应的认证重定向请求(authentication redirection request)(步骤S220)，从上述用户终端所执行的认证应用程序中获得质询开始请求信息(步骤S230)，则认证服务器生成与上述质询开始请求信息相对应的可变认证值，并向上述认证应用程序传递包含上述可变认证值的质询开始请求响应信息(步骤S235)，从而支援上述认证应用程序从上述服务提供服务器获得与用于判断作为上述服务提供服务器的认证书的服务器认证书是否有效的服务器质询请求信息(步骤S240)相对应的服务器质询请求响应信息。

[0084] 其中，质询开始请求信息可以包含能够识别应用程序认证书的应用程序认证书识

别信息、上述服务提供应用程序识别信息、上述推荐人服务密钥中的至少一个。

[0085] 与此相对应的质询开始请求响应信息还可以包含上述推荐人认证密钥及上述推荐人服务密钥中的至少一个信息。如上所述，上述推荐人认证密钥为在用户利用本发明的登录取代方法的过程中，为了识别是通过哪个认证应用程序，哪个服务提供服务器进行传递的质询开始请求，即，为了识别认证应用程序及服务提供服务器而通过上述认证服务器提供的值。

[0086] 然后，本发明第一实施例的多重签名登录取代方法还包括步骤S250，即，如果从上述认证应用程序获得响应请求信息，上述响应请求信息包含作为利用作为上述认证应用程序的认证书的应用程序认证书的私钥(private key)对上述服务器质询请求响应信息进行签名的值的多重签名值，则上述认证服务器利用上述响应请求信息判断上述服务器认证书及上述应用程序认证书是否有效。

[0087] 其中，上述响应请求信息还可以包含上述推荐人认证密钥、上述服务类型信息、上述授权级别及服务提供服务器识别信息中的至少一个。

[0088] 上述步骤(S250)的特征在于，上述认证服务器利用上述服务器认证书的公钥及上述应用程序认证书的公钥验证上述多重签名值的签名，从而判断上述服务器认证书及上述应用程序认证书是否有效。在这种情况下，可以从上述多重签名值中利用上述服务器认证书的公钥及上述应用程序认证书的公钥获得预定的哈希值(A)，并对在上述哈希值(A)和上述可变认证值中适用预定的哈希函数获得的结果值(B)进行比较，从而可以验证签名的有效性。在这种比较中，如果适用上述哈希值和上述预定的哈希函数获得的结果值不同，则签名为无效，如果相同，则签名为有效，这与普通技术人员所公知的内容相同，普通技术人员可以很好地理解用于验证签名(在此为电子签名)的有效性的方法。

[0089] 另一方面，与上述步骤S250相关地，上述认证服务器的特征在于，可以管理涉及针对上述服务提供服务器的访问级别(access level)的信息或者可以支援进行管理，并可以参照上述访问级别决定授权级别(authorization level)，在这种情况下，上述认证结果消息包含涉及上述授权级别的信息，而上述服务器认证书是否有效则参照上述授权级别进行判断。

[0090] 例如，访问级别有可能是与上述服务提供服务器是否被入侵(cracking)过，如果有，那么次数和频率是如何等相关的入侵履历信息，或者如上述服务提供服务器所能够提供的安保服务的功能和性能之类的信息及基于上述许可证级别指定的等级信息。如与上述的认证书的注册阶段相关的例示所示，上述访问级别可以为在认证书的注册阶段所指定的值，但并不局限于此，普通技术人员可以理解访问级别为可以根据时期而有所不同的值。

[0091] 另一方面，例如，在通过上述服务提供服务器向利用服务的用户允许的服务根据服务利用等级而得到区别化的情况下，根据上述访问级别指定的授权级别可以与表示其服务利用等级的信息相对应。并且，授权级别可以被用作决定可以通过一次登录利用服务的有效时间的基础。并且，认证服务器的运营人员可以在服务提供服务器因暴露在入侵中等理由而在其登录取代服务方面需要进行制约的情况下，可以很容易变更访问级别或者授权级别。

[0092] 然后，本发明第一实施例的多重签名登录取代方法还包括步骤S260a、步骤S260b及步骤S270，即，上述认证服务器向上述认证应用程序及上述服务提供服务器中的至少一

个传递包含上述服务器认证书是否有效的认证结果消息(步骤S260a、步骤S260b),从而在上述认证结果消息为表示上述服务器认证书有效的认证成功消息的情况下,支援上述服务提供服务器向上述用户终端所执行的服务提供应用程序传递预定的访问令牌(access token)(步骤S270),从而支援上述服务提供应用程序能够通过上述访问令牌利用上述服务,由此对上述登录进行处理。在图2的序列图中,虽然以在步骤S260a之后进行步骤S260b的方式进行了图示,但这一顺序可以相反,并且,步骤S260a和步骤S260b可以同时执行。

[0093] 另一方面,本发明第一实施例的多重签名登录取代方法可以在上述步骤S250之后还包括上述认证服务器在上述区块链数据库记录上述认证结果消息或者对此进行加工的值作为认证结果事务,或者支援与上述认证服务器相联动的其他装置进行记录的步骤(未图示)。通过在区块链数据库记录上述认证结果事务,不仅可以使利用认证服务器的管理人员或者具有可以访问上述区块链数据库的权限的第三人验证上述认证结果消息的真假,而且可以管理多个认证结果消息的统计数值等。

[0094] 并且,本发明第一实施例的多重签名登录取代方法还可以包括响应周期性(periodically)或者完整性验证请求,在上述认证服务器参照记录于上述区块链数据库的(i)特定服务器认证书的信息或者作为对此进行加工后的值的特定服务器认证书注册事务,(ii)特定应用程序认证书的信息或者作为对此进行加工后的值的特定应用程序认证书注册事务,以及(iii)特定认证结果消息或者作为对此进行加工后的值的特定认证结果事务中的至少一个信息验证上述(i)、(ii)、(iii)的信息的完整性(integrity),或者支援与上述认证服务器相联动的其他装置进行验证的步骤(未图示)。

[0095] 然后,图3为以例示性的方式表示根据本发明在没有用户ID的状态下利用多重信息取代登录的方法(以下称为“临时ID登录取代方法”)的序列图。以下,将不再反复说明与上述的第一实施例的多重签名登录取代方法相同的细节特征,仅具体说明不同之处。

[0096] 参照图3,本发明第一实施例的临时ID登录取代方法包括步骤S310至步骤S330,即,如果从上述第二应用程序中获得包含用于识别用户的用户识别信息的认证请求信息(步骤S320),上述第二应用程序从用户终端所执行的第一应用程序中接收作为通过上述用户终端所执行的第二应用程序请求取代登录的信息的认证重定向请求(authentication redirection request)(步骤S310),则上述服务提供服务器向认证服务器传递包含上述用户识别信息的质询开始请求信息(步骤S330)。

[0097] 其中,用户识别信息作为用于将上述用户与其他用户区别进行识别的信息,只要每个用户为以独一无二(unique)的方式指定的信息就无妨。例如,用户识别信息既可以为用于利用通过上述第二应用程序提供的服务的登录信息,也可以为针对上述用户进行发放的预定的认证书信息。

[0098] 并且,与第一实施例的多重签名登录取代方法类似,上述步骤S310至步骤S330的特征在于,可以在上述区块链数据库中记录作为上述服务提供服务器的认证书的服务器认证书的信息或者作为对此进行加工后的值的服务器认证书注册事务,以及作为上述第二应用程序的认证书的应用程序认证书的信息或者作为对此进行加工的值的应用程序认证书注册事务的状态执行。

[0099] 然后,本发明第一实施例的临时ID登录取代方法还包括步骤S335、步骤S340,即,如果响应上述质询开始请求信息获得包含通过上述认证服务器生成的可变认证值的质询

开始请求响应信息(步骤S335)，则上述服务提供服务器向上述第二应用程序传递包含上述可变认证值的应用程序质询请求信息(步骤S340)，从而支援上述第二应用程序生成利用作为上述第二应用程序的认证书的应用程序认证书的私钥(private key)对上述可变认证值进行签名的值。

[0100] 作为适用于本发明所利用的基于PKI的加密方式的一例示，上述质询开始请求信息还可以包括作为上述服务提供服务器的认证书的服务器认证书的公钥，在这种情况下，上述质询开始请求响应信息可以包含通过上述服务器认证书的公钥编码的上述可变认证值。这时，就上述例示而言，在上述步骤S335、步骤S340中，上述服务提供服务器可以利用上述服务器认证书的私钥(private key)从上述质询开始请求响应信息(步骤S335)中获得上述可变认证值，并且，可以向上述第二应用程序传递包含利用上述应用程序认证书的公钥对上述可变认证值进行签名的值的上述应用程序质询请求信息(步骤S340)。

[0101] 重新参照图3，在上述步骤S335步骤S340之后，本发明第一实施例的临时ID登录取代方法还包括步骤S345、步骤S350，即，如果获得包含利用上述应用程序认证书的私钥(private key)进行签名的值的应用程序质询请求响应信息(步骤S345)，则上述服务提供服务器向上述认证服务器传递上述应用程序质询请求响应信息(步骤S350)，从而支援上述认证服务器利用上述应用程序质询请求响应信息判断上述应用程序认证书是否有效。

[0102] 由于上述应用程序质询请求响应信息包含利用上述应用程序认证书的私钥签名的值，因此，可以利用上述认证服务器所拥有的上述应用程序认证书的公钥验证其所签名的值是否为与上述可变认证值相对应的值，由此能够判断上述应用程序认证书是否有效。对此的说明将利用上述的与对签名的有效性进行验证的方法相关的说明进行替代。

[0103] 在上述步骤S345、步骤S350之后，本发明第一实施例的临时ID登录取代方法还包括从上述认证服务器中获得包含上述应用程序认证书是否有效的认证结果消息，并且，上述认证结果消息表示上述应用程序认证书有效的认证成功消息，则上述服务提供服务器向上述第二应用程序传递临时ID(temporary ID)，从而支援上述第一应用程序能够通过从上述第二应用程序向上述第一应用程序传递的(i)上述临时ID及(ii)上述认证成功消息所包含的访问令牌(access token)利用上述服务，由此对上述登录进行处理的步骤。

[0104] 其中，可以参照上述认证成功消息所包含的访问令牌及授权级别相关信息决定临时ID。例如，可以向上述临时ID赋予表示能够与上述服务提供服务器所提供的服务的特性相匹配地进行利用的服务的与服务利用等级相关的信息，具有上述临时ID并通过第一应用程序利用上述服务的用户也可以根据服务利用等级在指定的范围内利用服务。

[0105] 如果以认证服务器为基准对上述的本发明第一实施例的临时ID登录取代方法进行重新说明如下，临时ID登录取代方法包括：步骤S310至步骤S330，即，首先，从用户终端所执行的第一应用程序向上述第二应用程序传递作为通过上述用户终端所执行的第二应用程序请求取代登录的信息的认证重定向请求(authentication redirection request)(步骤S310)，从上述第二应用程序向上述服务提供服务器传递包含有用于识别用户的用户识别信息的认证请求信息(步骤S320)，如果从上述服务提供服务器获得包含上述用户识别信息的质询开始请求信息(步骤S330)，则认证服务器响应上述质询开始请求信息生成可变认证值；步骤S335、步骤S340，即，向上述服务提供服务器传递包含所生成的上述可变认证值的质询开始请求响应信息(步骤S335)，从而支援上述服务提供服务器向上述第二应用程序

传递包含上述可变认证值的应用程序质询请求信息(步骤S340),并支援上述第二应用程序生成利用作为上述第二应用程序的认证书的应用程序认证书的私钥(private key)对上述可变认证值进行签名的值;以及步骤S345、步骤S350,如果获得包含利用上述应用程序认证书的私钥(private key)进行签名的值的应用程序质询请求响应信息(步骤S345、步骤S350),则上述认证服务器利用上述应用程序质询请求响应信息判断上述应用程序认证书是否有效。

[0106] 与第一实施例的多重签名登录取代方法类似,第一实施例的临时ID登录取代方法还可以包括上述认证服务器在上述区块链数据库记录上述认证结果消息或者对此进行加工的值作为认证结果事务,或者支援与上述认证服务器相联动的其他装置进行记录的步骤(未图示)。

[0107] 重新参照图3,第一实施例的临时ID登录取代方法在步骤S345、步骤S350之后还包括步骤S355a至步骤S370b,即,上述认证服务器向上述服务提供服务器及上述第二应用程序传递包含上述应用程序认证书是否有效的认证结果消息(步骤S355a、步骤S355b),从而支援上述服务提供服务器在上述认证结果消息为表示上述应用程序认证书有效的认证成功消息的情况下,向上述第二应用程序传递临时ID(temporary ID)(步骤S360),并支援上述第一应用程序能够通过从上述第二应用程序向上述第一应用程序传递的(i)上述临时ID(步骤S360、步骤S370a)及(ii)上述认证成功消息所包含的访问令牌(access token)(步骤S355b、步骤S370b)利用上述服务(步骤S380),由此对上述登录进行处理。在图3的序列图中,虽然以在步骤S355a后面执行步骤S355b的方式进行了图示,但这种顺序可以相反,并且,步骤S355a和步骤S355b也可以同时执行。步骤370a和步骤S370b也与此相同。

[0108] 另一方面,第一实施例的临时ID登录取代方法还可以包括响应周期性(periodically)或者完整性验证请求,上述认证服务器参照记录于上述区块链数据库的(i)特定服务器认证书的信息或者作为对此进行加工后的值的特定服务器认证书注册事务,(ii)特定应用程序认证书的信息或者作为对此进行加工后的值的特定应用程序认证书注册事务,以及(iii)特定认证结果消息或者作为对此进行加工后的值的特定认证结果事务中的至少一个信息,从而验证上述(i)、(ii)、(iii)的信息的完整性(integrity),或者支援与上述认证服务器相联动的其他装置进行验证的步骤(未图示)。

[0109] 第二实施例

[0110] 然后,对涉及本发明的登录取代方法的第二实施例进行说明。以下,将不再继续反复说明与上述第一实施例相同的技术特征,仅具体说明不同之处。

[0111] 重新参照图2,涉及第一实施例进行叙述的步骤S210、步骤S215,在本发明第二实施例的多重签名登录取代方法中,在以下状态下执行:对与作为上述服务提供服务器的认证书的服务器认证书的信息或者作为对此进行加工后的值的服务器认证书注册事务的哈希值的第一特定哈希值相匹配的至少一个相邻哈希值一同进行哈希计算所生成的第一代表哈希值或者对上述第一代表哈希值进行加工的值,其中,上述相邻哈希值为包含(i)特定服务器认证书的信息或者作为对此进行加工后的值的特定服务器认证书注册事务的哈希值,(ii)特定应用程序认证书的信息或者作为对此进行加工后的值的特定应用程序认证书注册事务的哈希值,以及(iii)特定认证结果消息或者作为对此进行加工后的值的特定认证结果事务的哈希值的多个哈希值中的一个,以及对与作为用户终端所执行的认证应用程

序的认证书的应用程序认证书注册事务的哈希值的第二特定哈希值相匹配的至少一个上述相邻哈希值一同进行哈希计算所生成的第二代表哈希值或者对上述第二代表哈希值进行加工的值被记录于预定的区块链数据库。

[0112] 之后，在步骤S230、步骤S235中，上述认证服务器在判断上述服务器认证书及上述应用程序认证书是否有效时参照上述预定的区块链数据库。其具体意义为，利用参照上述预定的区块链数据库获得的上述服务器认证书注册事务及上述应用程序认证书注册事务判断上述服务器认证书及上述应用程序认证书是否有效。

[0113] 这种本发明的第二实施例能够以锚固(anchoring)方式构成，上述锚固(anchoring)方式在第二区块链数据库记录利用虚拟货币的UTXO在第一区块链数据库记录涉及其UTXO的个别事务之后，在第二区块链数据库记录被记录于上述第一区块链数据库的多个事务生成的代表哈希值，从而以双重方式谋求记录的完整性，而在这种情况下，上述预定的区块链数据库为第二区块链数据库，步骤S210、步骤S215则在上述服务器认证书注册事务及上述应用程序认证书注册事务追加记录于第一区块链数据库的状态下执行。

[0114] 对上述锚固方式进一步具体说明如下：在本发明第二实施例的多重签名登录取代方法中，在步骤S250之后，还可以包括执行如下过程的步骤(未图示)，即，(A)上述认证服务器在上述第一区块链数据库记录上述认证结果消息或者对此进行加工的值作为认证结果事务，或者支援与上述认证服务器相联动的其他装置进行记录的过程；以及(B)如果满足至少一个锚固条件，则在上述第二区块链数据库记录对与作为上述认证结果事务的哈希值的特定哈希值相匹配的至少一个相邻哈希值一同进行哈希计算生成的代表哈希值或者对上述代表哈希值进行加工的值，其中，上述相邻哈希值为包含(i)特定服务器认证书的信息或者作为对此进行加工后的值的特定服务器认证书注册事务的哈希值，(ii)特定应用程序认证书的信息或者作为对此进行加工后的值的特定应用程序认证书注册事务的哈希值，以及(iii)特定认证结果消息或者作为对此进行加工后的值的特定认证结果事务的哈希值的多个哈希值中的一个，或者支援与上述认证服务器相联动的其他装置进行记录，并执行获得作为上述代表哈希值或者对上述代表哈希值进行加工的值被记录于上述第二区块链数据库的位置信息的事务ID的过程。

[0115] 此时，上述的锚固条件可以包括：(i)获得或者生成与预定的数量相对应的上述特定哈希值和相邻哈希值的条件，(ii)经过预定时间的条件，(iii)在上述第一区块链数据库生成块的条件，(iv)针对服务特性的条件中的至少一个。

[0116] 特定哈希值和至少一个相邻哈希值的计算可以通过多种函数执行。当表示特定哈希值为input，至少一个相邻哈希值为x1、x2、…、xn时，代表哈希值t能够以如下数学式表示。

[0117] [数学式1]

[0118] t＝hash(function(input,x1,x2,...,xn))

[0119] 此时，认证服务器可以将上述特定哈希值和上述至少一个相邻哈希值作为预定的数据结构进行存储和管理。其中，数据结构可以多种多样，作为一例，也可以为梅克尔树(merkle tree)结构。在这种情况下，上述特定哈希值和至少一个相邻哈希值的计算可以通过梅克尔树实现。

[0120] 即，上述认证服务器可以使上述特定哈希值生成被分配于叶节点的梅克尔树

(merkle tree),或者支援其生成,并且,如果满足至少一个上述锚固条件,则可以获得对被分配于与上述特定哈希值相匹配的至少一个另一叶节点的哈希值一同进行哈希计算所生成的上述代表哈希值或者对上述代表哈希值进行加工的值,并在上述第二区块链数据库记录所获得的上述值,或者支援其他装置进行记录。

[0121] 上述认证服务器最终将作为被分配于梅克尔树的根节点的哈希值作为代表哈希值记录于上述第二区块链数据库,或者支援其他装置进行记录。此时,可以记录对代表哈希值进行加工后的值。例如,可以在代表哈希值注册已执行hex计算的结果值。

[0122] 另一方面,在上述认证服务器存储上述特定哈希值和上述至少一个相邻哈希值作为预定的第一数据结构,之后存储与上述第一数据结构相同形态的第二数据结构进行管理的情况下,上述第一数据结构和上述第二数据结构能够以链条形态相连接。

[0123] 尤其,如上述例所示,在上述第一数据结构及上述第二数据结构为梅克尔树的情况下,上述第一数据结构的根值或者上述根值的哈希值可以被分配于上述第二数据结构的第一个叶节点。

[0124] 并且,当生成第二数据结构时,实现对第一数据结构的验证,从而可以更进一步确切地保证数据的完整性。

[0125] 并且,在上述梅克尔树为以链条形态相连接的至少一个梅克尔树中属于第一个梅克尔树的情况下,可以在上述梅克尔树的第一个叶节点分配由文本、数字或者记号所形成的预定的消息数据的哈希值或者对此进行加工的值。例如,当生成梅克尔树时,可以分配通过认证服务器最初赋予的输入消息的哈希值。

[0126] 图4及5为示出根据本发明生成的梅克尔树的例的图。

[0127] 在图4中,示出叶节点的数量为4(2^2)个的梅克尔树。由于所图示的梅克尔树为第一个梅克尔树(tree_id＝0),因此,可知在作为第一个叶节点的h1节点分配有预定的消息数据PrivBC_unique_message的哈希值SHA256(PrivBC_unique_message)。在具有多个事务的注册的情况下,上述认证服务器生成当前构成中的梅克尔树的最后叶节点之后的叶节点分配特定哈希值或者对特定哈希值进行加工的值,或者支援其他装置进行分配。例如,在图4的梅克尔树中,在之前的步骤结束直到作为第二个叶节点的h1节点为止的值的分配的情况下,生成之后的叶节点的h2节点分配特定哈希值或者对特定哈希值进行加工的值(SHA256(input2))。并且,上述认证服务器可以计算(i)特定哈希值,以及(ii)被分配于作为分配有上述特定哈希值的第三叶节点的h2节点的同级节点h3节点的哈希值,或者支援其他装置进行计算。针对作为上述计算的结果的计算值的哈希值被分配于h2节点和h3节点的父节点(h23节点)。由于父节点(h23节点)并非为梅克尔树的根节点,因此,上述认证服务器可以使用被分配于上述h23节点的哈希值作为上述特定哈希值反复执行上述过程。即,可以将被分配于h23节点的哈希值作为特定哈希值,并对分配于h23节点的哈希值和分配于h01节点的哈希值进行计算以分配于h23节点和h01节点的父节点(h0123)。此时,由于h0123节点为梅克尔树的根节点,因此,上述认证服务器可以在第二区块链数据库记录被分配于h0123节点的哈希值或者对此进行加工的值(hex(h{node_index})),或者支援其他装置进行记录。

[0128] 以递归(recursive)方式对此进行说明如下:当满足至少一个上述锚固条件时,(x1)上述认证服务器对(i)上述特定哈希值和(ii)被分配于分配有上述特定哈希值的节点

的同级节点的哈希值一同进行哈希计算,或者支援其他装置进行哈希计算,并在上述节点的父节点分配作为上述计算的结果的计算值的哈希值,或者支援其他装置进行分配;(x2)如果上述父节点为上述梅克尔树的根节点,则在上述第二区块链数据库记录分配于上述父节点的哈希值作为上述代表哈希值,或者支援其他装置进行记录;(x3)如果上述父节点并非为上述梅克尔树的根节点,则将分配于上述父节点的哈希值作为上述特定哈希值反复执行上述(x1)至(x3)。

[0129] 在第二实施例中,以与叶节点的数量相对应地获得多个哈希值,则各个哈希值可以成为上述的梅克尔树的输入值(分配于叶节点的值),其中,上述哈希值为(i)特定服务器认证书的信息或者作为对此进行加工后的值的特定服务器认证书注册事务的哈希值,(ii)特定应用程序认证书的信息或者作为对此进行加工后的值的特定应用程序认证书注册事务的哈希值,以及(iii)特定认证结果消息或者作为对此进行加工后的值的特定认证结果事务的哈希值。

[0130] 并且,认证服务器可以按预定时间单位生成上述的梅克尔树的根值(上述(ii)锚固条件)。在这种情况下,如果经过预定的时间,则上述认证服务器可以利用到那时为止的输入值生成梅克尔树,并且在第二区块链数据库中记录梅克尔树的根值,或者支援其他装置进行记录。

[0131] 但是,在这种情况下,即使经过了预定时间,也有可能未在分配有梅克尔树的特定哈希值的节点的同级节点分配值。像这样,即使满足了预定的上述锚固条件,也未在分配有上述特定哈希值的节点的同级节点分配哈希值的情况下,上述认证服务器在上述同级节点分配预定的哈希值,或者支援其他装置进行分配,从而能够以上述的方式计算出梅克尔树的根值。例如,上述认证服务器可以复制上述特定哈希值分配于上述同级节点,或者支援其他装置进行分配。

[0132] 并且,上述服务特性可以为利用登录取代服务的多个实体(entity)所支付的费用信息、实现上述事务的记录的时间段信息、实现上述记录的区域信息及作为参与上述记录的服务器的管理主体的公司类型信息中的至少一部分。只不过,并不局限于在此所记载的内容。

[0133] 另一方面,如果开始生成新的梅克尔树,并且在没有接收事务的状态下满足至少一个上述anchoring条件,则上述认证服务器生成预定的消息数据被分配于第一个叶节点和第二个叶节点的梅克尔树,或者支援其他装置生成,并且,在第二区块链数据库记录上述梅克尔树的根值或者对此进行加工的值,或者支援其他装置进行记录。例如,在这样的情况下,可以生成叶节点为两个的梅克尔树。

[0134] 另一方面,如上所述,在认证服务器存储上述特定哈希值和上述至少一个相邻哈希值作为预定的第一数据结构,之后存储与上述第一数据结构相同形态的第二数据结构进行管理的情况下,上述第一数据结构和上述第二数据结构能够以链条形态相连接。尤其,在上述第一数据结构及上述第二数据结构为梅克尔树的情况下,上述第一数据结构的根值或者上述根值的哈希值可以被分配于上述第二数据结构的第一个叶节点。

[0135] 图5为示出根据本发明以上述第二数据结构生成的梅克尔树的图。

[0136] 参照图5,可知图4的梅克尔树(tree_id=0)的根值(hex(h0123))被分配于新的梅克尔树的第一个叶节点(h4节点)。本发明具有如下优点:像这样,通过连接在发生事务时所

生成的多个数据结构，从而即使在中间发生数据变造的情况下，也可以轻易实现跟踪，从而提高数据的完整性。

[0137] 并且，本发明第二实施例的认证书的注册方法还包括响应周期性(periodically)或者完整性验证请求，上述认证服务器验证与被记录于上述第一区块链数据库的至少一个事务的哈希值相匹配的至少一个上述相邻哈希值一同进行哈希计算所生成的第一代表哈希值或者对上述第一代表哈希值进行加工的值与被记录在与此相对应的上述第二区块链数据库的第二代表哈希值或者对上述第二代表哈希值进行加工的值是否一致，从而验证上述事务的完整性(integrity)，或者支援与上述认证服务器相联动的其他装置进行验证的步骤(未图示)，其中，上述事务为包含(i)特定服务器认证书的信息或者作为对此进行加工后的值的特定服务器认证书注册事务，(ii)特定应用程序认证书的信息或者作为对此进行加工后的值的特定应用程序认证书注册事务，以及(iii)特定认证结果消息或者作为对此进行加工后的值的特定认证结果事务的多个事务中的一个。

[0138] 作为一例示，上述第一及第二区块链数据库可以为区块链数据库。此时，上述第一区块链数据库可以为私人(private)区块链数据库，上述第二区块链数据库可以为公共(public)区块链数据库。

[0139] 只不过，本发明并不局限于此，普通技术人员可以很好地理解上述第一区块链数据库可以为私人区块链数据库或者公共区块链数据库，同样，上述第二区块链数据库可以为私人区块链数据库和公共区块链数据库中的一个。

[0140] 然后，将对第二实施例的临时ID登录取代方法进行说明，但不再反复说明与上述第一实施例相同的技术特征，仅具体说明不同之处。

[0141] 参照图3，涉及第一实施例进行叙述的步骤S310至步骤S330，在本发明第二实施例的临时ID登录取代方法中，在以下状态下执行：对与作为用户终端所执行的第二应用程序的认证书的应用程序认证书的信息或者作为对此进行加工的值的应用程序认证书注册事务的哈希值的特定哈希值相匹配的至少一个相邻哈希值一同进行哈希计算生成的代表哈希值或者上述代表哈希值进行加工后的值记录于预定的区块链数据库，其中，上述相邻哈希值为包含(i)特定应用程序认证书的信息或者作为对此进行加工后的值的特定应用程序认证书注册事务的哈希值及(ii)特定认证结果消息或者作为对此进行加工后的值的特定认证结果事务的哈希值的多个哈希值中的至少一个。另一方面，通过上述认证服务器参照上述预定的区块链数据库判断上述应用程序认证书是否有效。

[0142] 并且，与第二实施例的多重签名登录取代方法类似，第二实施例的临时ID登录取代方法还可以包括上述认证服务器执行包括如下过程的步骤(未图示)：(A)将上述认证结果消息或者对此进行加工的值作为认证结果事务记录于上述第一区块链数据库，或者支援与上述认证服务器相联动的其他装置进行记录的过程；以及(B)如果满足至少一个锚固条件，则在上述第二区块链数据库记录对与作为上述认证结果事务的哈希值的特定哈希值相匹配的至少一个相邻哈希值一同进行哈希计算生成的代表哈希值或者对上述代表哈希值进行加工的值，或者支援与上述认证服务器相联动的其他装置进行记录，并且，获得作为上述代表哈希值或者对上述代表哈希值进行加工的值被记录于上述第二区块链数据库的位置信息的事务ID的过程的步骤(未图示)，其中，上述相邻哈希值包含(i)特定应用程序认证书的信息或者作为对此进行加工后的值的特定应用程序认证书注册事务的哈希值及(ii)

特定认证结果消息或者作为对此进行加工后的值的特定认证结果事务的哈希值中的至少一个。

[0143] 不同于第二实施例的多重签名登录取代方法,在第二实施例的临时ID登录取代方法中,并非必须在相邻哈希值中包含特定服务器认证书的信息或者作为对此进行加工后的值的特定服务器认证书注册事务,这是因为服务器认证书并非必须使用的。除去这种不同之处,在第二实施例的多重签名登录取代方法中说明的内容也可以适用于第二实施例的临时ID登录取代方法。

[0144] 第三实施例

[0145] 然后,对涉及本发明的登录取代方法的第三实施例进行说明。以下,仅说明不同于上述第一实施例的第三实施例的技术特征。

[0146] 第三实施例的方法利用智能合约执行。上述智能合约为可以被可执行的字节码编译,并在包括认证服务器或者与上述认证服务器相联动的其他装置的多个计算装置上执行的源代码,当进行上述执行时,如果满足特定条件,则执行预先指定的程序,而作为上述执行的结果的执行结果值的完整性(integrity)则通过从上述多个计算装置中计算出的上述执行结果值的一致性(consensus)得到验证。

[0147] 基于上述智能合约的认证书的信息包含(i)通过基于上述公钥基础设施(public key infrastructure,PKI)的加密方式生成的公钥(public key)PubA,以及(ii)作为与上述认证书的有效条件VcertA相对应的智能合约SC(VcertA)被编译(compile)后的结果的字节码BC(SC(VcertA))。基于上述智能合约的认证书的信息还可以包含(iii)作为对用于识别上述认证书的利用主体的识别信息进行哈希计算的结果值的识别信息哈希值IdhashA。并且,基于上述智能合约的认证书的信息还可以包含加密类型(crypto type)、许可证密钥(license key)、许可证级别(license level)之类的追加性的信息中的至少一个作为用于对基于上述PKI的加密方式的种类及所示哈希计算的种类中的至少一个进行特定的信息。

[0148] 这种认证书的信息可以为获得与认证书的利用主体相对应的公钥(public key)PubA、作为对用于识别认证书的利用主体的识别信息进行哈希计算的结果值的识别信息哈希值IdhashA及上述认证书的有效条件VcertA(步骤S205及步骤S210)的认证服务器或者其他装置生成与有效条件相对应的上述智能合约SC(VcertA),并且,对上述智能合约进行编译(compile),从而生成作为其结果的字节码BC(SC(VcertA))而获得的。

[0149] 在上述第三实施例中,作为上述服务提供服务器的认证书的服务器认证书及作为用户终端所执行的认证应用程序的认证书的应用程序认证书可以为基于上述智能合约的认证书。

[0150] 具体地,重新参照图2,涉及第一实施例进行叙述的步骤S210、步骤S215,在本发明第三实施例的多重签名登录取代方法中,在上述服务器认证书的信息或者作为对此进行加工后的值的服务器认证书注册事务或者上述应用程序认证书的信息或者作为对此进行加工的值的应用程序认证书注册事务被记录于上述区块链数据库,作为上述服务器认证书及上述应用程序认证书的上述智能合约SC(VcertA)的执行参数的状态S(SC(VcertA))被记录于状态数据库(state database)SDB的状态下执行。当包含上述智能合约的服务器认证书及应用程序认证书最初被记录时,上述S(SC(VcertA))被设定为预定的初始状态(initial state)记录于状态数据库。其中,上述初始状态意味着为了判断是否满足上述有效条件而

针对认证书最初提供的状态，例如，与图7的智能合约相对应的初始状态为counter＝10。

[0151] 之后，在步骤S230、步骤S235中，上述认证服务器在判断上述服务器认证书及上述应用程序认证书是否有效的过程中参照预定的区块链数据库及上述状态数据库。其具体含义为，参照(i)通过参照上述预定的区块链数据库获得的上述服务器认证书注册事务，(ii)上述应用程序认证书注册事务，(iii)从上述状态数据库获得的上述服务器认证书及上述应用程序认证书各自的智能合约的现有执行结果值及(iv)它们的新的执行结果值判断上述服务器认证书及上述应用程序认证书是否有效。为了参照上述预定的区块链数据库，上述认证服务器还可以利用事务位置标识符，上述事务位置标识符参照在分别注册上述服务器认证书注册事务及应用程序认证书注册事务时所获得的上述服务器认证书注册事务及应用程序认证书注册事务分别在上述预定的区块链数据库进行注册的位置。涉及判断认证书是否有效的更加具体的说明将与认证服务器相关地进行后述。其中，上述认证书的有效条件VcertA只要是基于通过上述智能合约能够获得的信息的条件，就可以包含任一种，但如果举出几种例示，那么就可以是基于(i)与上述利用主体的特征相关的信息，(ii)当使用上述认证书时的天气信息，(iii)当使用上述认证书时的日期信息，(v)作为与特定他人使用上述认证书相关的授权获得的信息，以及(iv)与预先指定的上述认证书的使用次数限制相关的信息中的至少一个的条件。其中，与利用主体的特征相关的信息例如，在利用主体为个人的情况下，意味着其个人的性别、身高、年龄等信息，这可以从执行智能合约的计算装置上的多个资源中获得。甚至，也可以包含于上述智能合约内。并且，在使用上述认证书时的日期信息也可以从互联网网站等所提供的数据中获得，上述(i)至(iv)的信息均可以从执行上述智能合约的多个计算装置上的多种资源中获得。

[0152] 根据这种上述有效条件VcertA构成上述智能合约的例示图示于图6及图7，图6及图7为以例示性的方式示出将上述认证书的使用次数分别限制在initNumber和10次的上述智能合约(源代码)的图。

[0153] 参照图6或者图7，公开了上述有效条件为认证书的使用次数限制在initNumber或者10次的智能合约的源代码。useCounter意味着向智能合约赋予的任意标题(title)，而相当于用于计算使用次数的计算器的状态的是被指定为int counter;的指令语，并且，在执行一次之后，通过被称为counter-＝1;的指令语发生变化的计数器的状态通过被称为return counter;的指令语得到返还。

[0154] 这种智能合约表示被转换为字节码且通过构成公共区块链数据库的多个计算装置(称为多个“节点”)执行的，其各自的执行结果可以通过一致性算法(consensus algorithm)使多个执行结果中占最多数的执行结果被验证为真正的执行结果。简单来讲，普通技术人员可以理解智能合约的执行结果的完整性是针对通过从多个上述节点中计算出的上述执行结果值的一致性(consensus)得到验证的。当然，根据情况，节点可以为一个，在这种情况下，一个计算装置也可以输出与这种一致性相匹配的验证结果。

[0155] 作为参考，图7所示的作为智能合约得到编译后的结构的字节码的例示如下。

[0156] 60606040525b600a600060005081905550 5b607e80601d6000396000f3606060405260006000357c0100000000000000000000000000000000000000000000000000000000900480 63d732d955146039576035565b6002565b6044600480505060 5a565b60405180828152602001915050604051809103 90f35b60006001600060008282825054039250508190555060006000505490

50607b565b9056。

[0157] 现在，具体说明在本发明第三实施例的多重签名登录取代方法的步骤S230、步骤S235中，上述认证服务器判断上述服务器认证书及上述应用程序认证书是否有效的方式。第三实施例的多重签名登录取代方法的步骤S230、步骤S235与第一实施例一样，包括上述认证服务器利用上述服务器认证书的公钥及上述应用程序认证书的公钥对上述多重签名值的签名进行验证的步骤。之后，在上述步骤S230、步骤S235中，还包括执行如下过程的步骤(未图示)，即，如果上述多重签名值的签名被验证为有效，则上述认证服务器执行(i)将作为上述服务器认证书所包含的上述智能合约的服务器认证书智能合约的状态S1作为执行参数执行上述服务器认证书智能合约的字节码BC1，或者支援与上述认证服务器相联动的其他装置执行，从而获得上述服务器认证书智能合约的执行结果值，并且参照上述服务器认证书智能合约的执行结果值判断上述服务器认证书是否有效的过程，以及(ii)将作为上述应用程序认证书所包含的上述智能合约的应用程序认证书智能合约的状态S2作为执行参数执行上述应用程序认证书智能合约的字节码BC2，或者支援与上述认证服务器相联动的其他装置执行，从而获得上述应用程序认证书智能合约的执行结果值，并且参照上述应用程序认证书智能合约的执行结果值判断上述应用程序认证书是否有效的过程。

[0158] 其中，由于在(i)过程为判断上述服务器认证书是否有效的过程，(ii)过程为判断上述应用程序认证书是否有效的过程这一点上相互对应，因此，以下以(i)过程为基准进行说明。

[0159] 在(i)过程中，如果举出图6级图7的例示说明将服务器认证书智能合约的状态S1作为执行参数执行上述服务器认证书智能合约的字节码BC1，并且参照上述服务器认证书智能合约的执行结果值判断上述服务器认证书是否有效的含义，则可以例举出0以上的整数counter为状态S1的执行参数作为与执行之前的状态相对应的认证书的剩余使用次数。如果剩余使用次数counter为0，则无法进一步使用认证书，因此，将此作为执行参数执行上述字节码BC1，从而获得未得到认证的执行结果值，例如counter＝-1，或者作为替代方案(alternatively)，即使不执行上述字节BC1，也可以从状态数据库获得无法得到认证的现有的执行结果值。除此之外，可以具有能够基于多种条件的执行参数计算出执行结果，从而参照上述执行结果判断认证书是否有效的诸多智能合约。

[0160] 如上所述，在利用认证书后，本发明第三实施例的多重签名登录取代方法可以在步骤S250之后还包括上述认证服务器执行如下过程的步骤(未图示)，即，(i)在上述区块链数据库记录上述认证结果消息或者对此进行加工的值作为认证结果事务，或者支援与上述认证服务器相联动的其他装置进行记录的过程，以及(ii)参照作为上述执行的结果获得的上述执行结果值，并将上述状态数据库的上述状态S(SC(VcertA))作为新的状态S’(SC(VcertA))在上述状态数据库中进行更新和注册，或者支援其他装置进行注册的过程。

[0161] 并且，本发明第二实施例的认证书的注册方法与第一实施例一样，不仅可以包括对特定服务器认证书注册事务、特定应用程序认证书注册事务、特定认证结果事务的完整性进行验证的步骤，而且追加地，还可以包括响应周期性(periodically)或者完整性验证请求，上述认证服务器参照被记录于上述状态数据库的个别智能合约的执行结果值，从而验证上述执行结果值的完整性，或者支援与上述认证服务器相联动的其他装置进行验证的步骤(未图示)。

[0162] 然后,对第三实施例的临时ID登录取代方法进行说明。参照图3,涉及第一实施例的临时ID登录取代方法进行叙述的步骤S310至步骤S330,在本发明第三实施例的临时ID登录取代方法中,在上述应用程序认证书的信息或者作为对此进行加工的值的应用程序认证书注册事务被记录于上述区块链数据库,作为上述应用程序认证书的上述智能合约SC(VcertA)的执行参数的状态(S(SC(VcertA))注册在状态数据库(state database)SDB的状态下执行。另一方面,通过上述认证服务器,并参照上述区块链数据库及上述状态数据库判断上述应用程序认证书是否有效。

[0163] 判断上述应用程序认证书是否有效的方式的关于基于智能合约的判断方式用关于根据第三实施例的多重签名登录取代方法进行说明的内容替代。

[0164] 另一方面,普通技术人员可以理解上述本发明的所有实施例既可以相互独立地实施,又可以相互组合实施。例如,第二实施例的多重签名登录取代方法可以与第三实施例的多重签名登录取代方法组合实施。在这种情况下,作为一个例示,可以从被记录于第三实施例的区块链数据库(第一区块链数据库)的个别事务的哈希值和被记录于状态数据库的值的哈希值构成梅克尔树,上述梅克尔树的代表哈希值可以被记录于第二实施例的第二区块链数据库。通过这种锚固,今后可以对利用被记录于第一区块链数据库的信息生成的哈希值和被记录于第二区块链数据库的代表哈希值进行相互比较,从而可以验证被记录于第一区块链数据库的内容的完整性。

[0165] 到目前为止所说明的本发明的所有实施例与以往的OAuth相比,具有不仅安全性和使用性得到了强化,而且还利用区块链数据库使得无法进行认证书的伪造变造的效果。

[0166] 作为上述实施例在此说明的技术的优点在于,事实上无法进行公钥、哈希值等与认证相关的信息的伪造变造,从而保证了认证书的可靠性,并且利用区块链数据库执行与认证相关的事务的验证,从而保证其完整性。

[0167] 基于上述实施例的说明,普通技术人员可以明确理解本发明可以通过软件及硬件的结合实现,或者仅通过硬件实现。贡献于本发明的技术解决方案的对象物或者现有技术的部分能够以可通过多种计算机结构要素执行的程序指令语的形态体现,从而记录于计算机可读记录介质。上述计算机可读记录介质可以单独或者组合包括程序指令语、数据文件、资料结构等。被记录于上述计算机可读记录介质的程序指令语既可以为为了本发明而特别设计和构成的,又可以为普通技术人员公知并能够使用的。计算机可读记录介质的例包括硬盘、软盘及磁带之类的磁介质、CD-ROM、DVD之类的光记录介质、光磁软盘(floptical disk)之类的磁光介质(magneto-optical media)及ROM、RAM、闪存之类的以存储和执行程序指令语的方式特别构成的硬件装置。程序指令语的例不仅包括由编译器所制作的机械代码,而且还包括可以使用解释器等通过计算机执行的高级语言代码。上述硬件装置能够执行本发明的处理而由一个以上的软件模块运行,反之也一样。上述硬件装置可以包括与用于存储程序指令语的ROM/RAM之类的存储器相结合,并构成为执行存储于上述存储器的多个指令语的CPU或者GPU之类的处理器,并且,可以包括能够与外部装置收发信号的通信部。并且,上述硬件装置可以包括用于接收由开发人员编写的多个指令语的键盘、鼠标及其他外部输入装置。

[0168] 以上,本发明通过具体构成要素等特定事项和受限的实施例及附图进行了说明,但这仅仅是为了帮助对本发明的进一步的理解而提供的,本发明并不局限于上述的多个实

施例，只要是本发明所属技术领域的普通技术人员，就可以从这样的记载中谋求多种修改及变形。

[0169] 因此，本发明的思想不应局限于上述所述的实施例，记载的权利要求范围，以及与上述权利要求范围均等地或者等同地发生变形的所有内容应属于本发明的思想范畴。

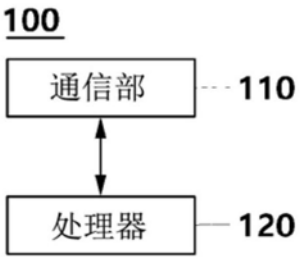

图1

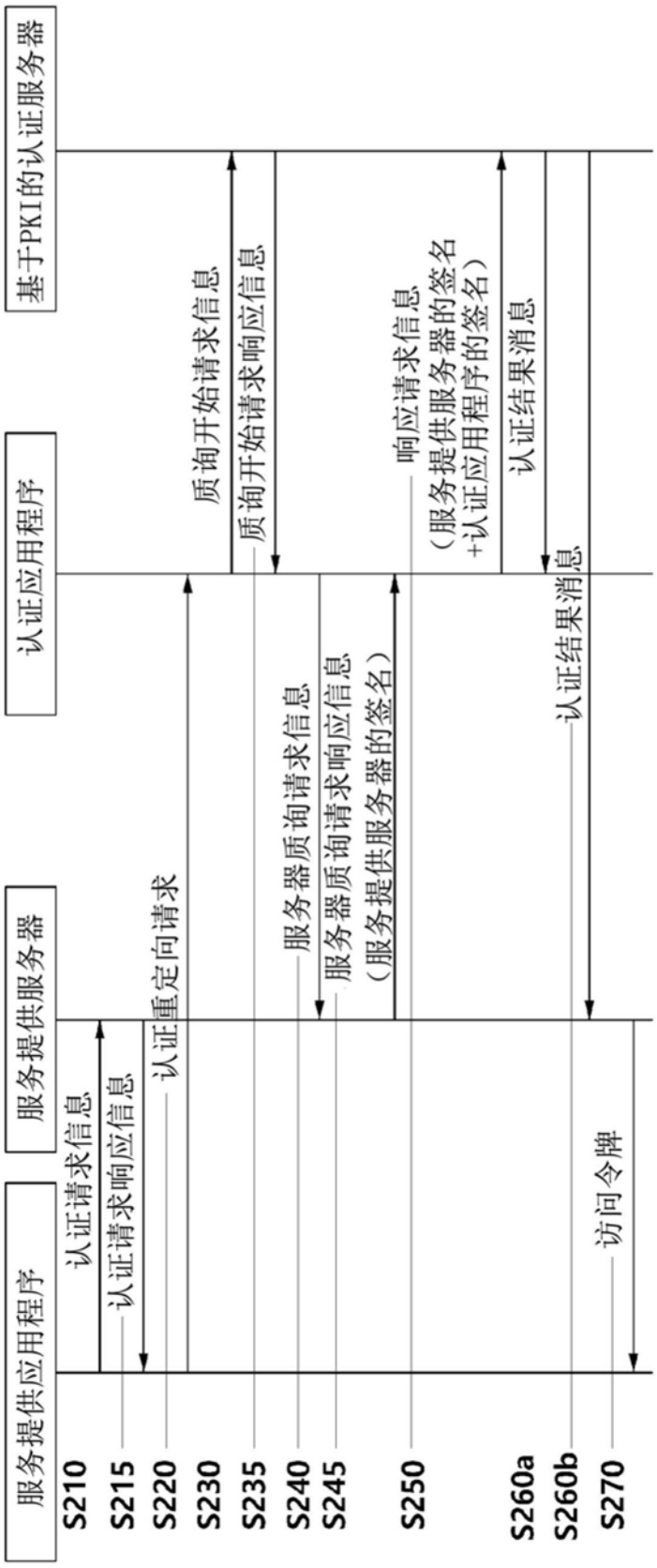
服务提供应用程序
服务提供服务器
认证应用程序
基于PKI的认证服务器
S210
认证请求信息
S215
认证请求响应信息
S220
认证重定向请求
S230
质询开始请求信息
S235
质询开始请求响应信息
S240
服务器质询请求信息
S245
服务器质询请求响应信息
（服务提供服务器的签名）
S250
响应请求信息
（服务提供服务器的签名
+认证应用程序的签名）
S260a
认证结果消息
S260b
认证结果消息
S270
访问令牌

图2

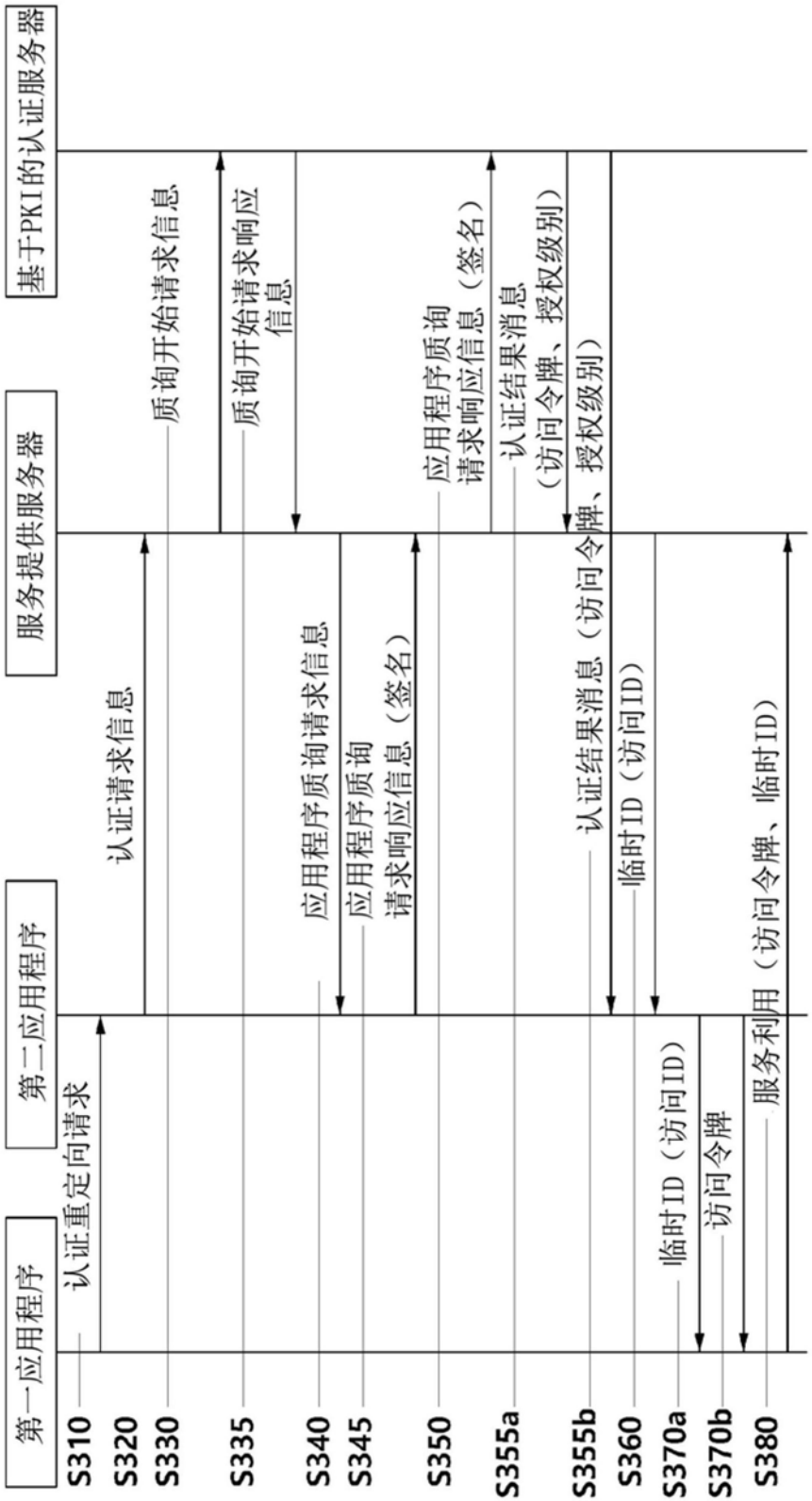
第一应用程序
第二应用程序
服务提供服务器
基于PKI的认证服务器
S310
认证重定向请求
S320
认证请求信息
S330
质询开始请求信息
S335
质询开始请求响应信息
S340
应用程序质询请求信息
S345
应用程序质询
请求响应信息（签名）
S350
应用程序质询
请求响应信息（签名）
S355a
认证结果消息
（访问令牌、授权级别）
S355b
认证结果消息（访问令牌、授权级别）
S360
临时ID（访问ID）
S370a
临时ID（访问ID）
S370b
访问令牌
S380
服务利用（访问令牌、临时ID）

图3

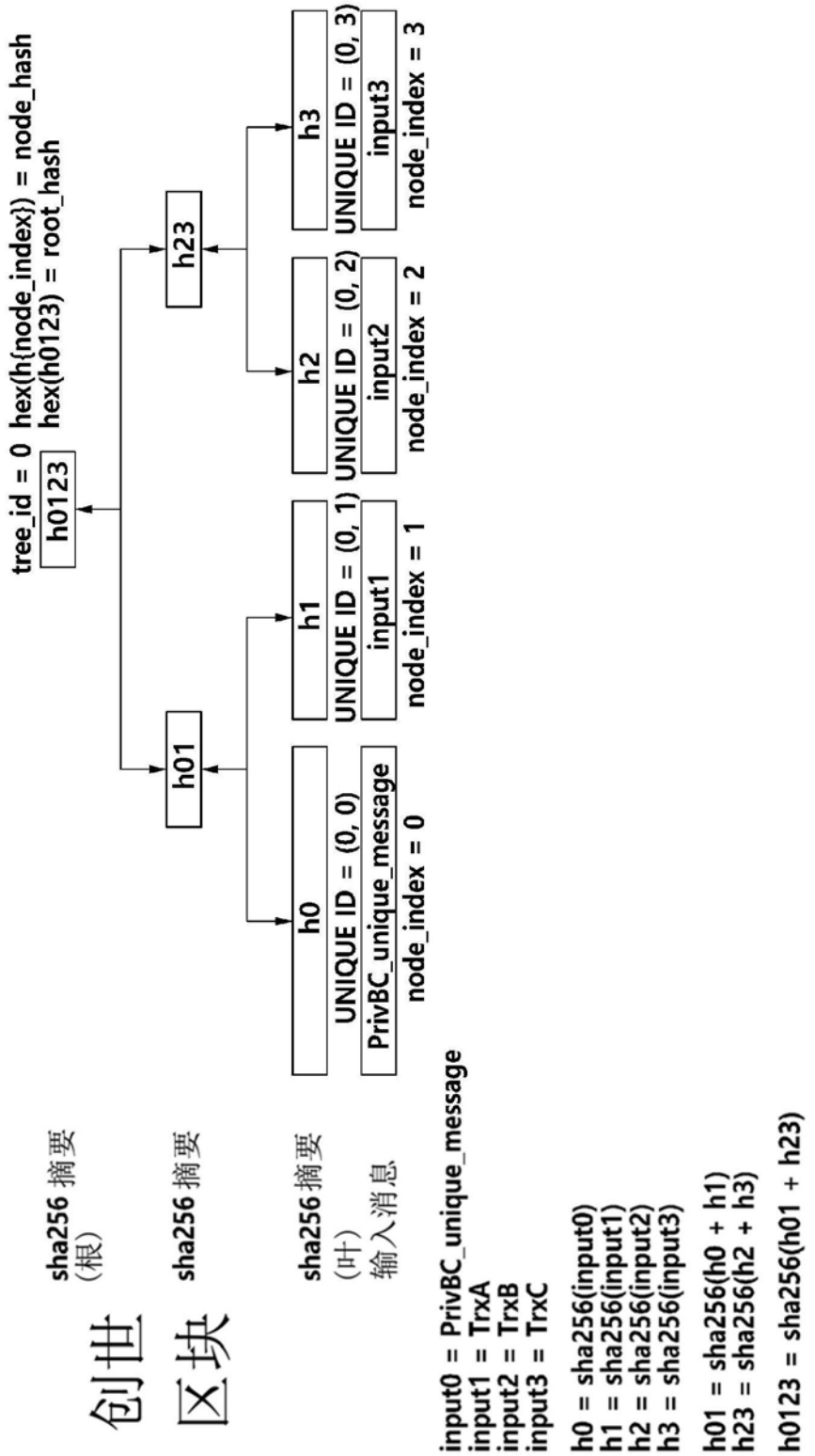
tree_id = 0 hex(h{node_index}) = node_hash
hex(h0123) = root_hash
h0123
h01
h23
h0
h1
h2
h3
UNIQUE ID = (0, 0)
UNIQUE ID = (0, 1)
UNIQUE ID = (0, 2)
UNIQUE ID = (0, 3)
PrivBC_unique_message
input1
input2
input3
node_index = 0
node_index = 1
node_index = 2
node_index = 3
sha256 摘要
(根)
sha256 摘要
sha256 摘要
(叶)
输入消息
创世区块
input0 = PrivBC_unique_message
input1 = TrxA
input2 = TrxB
input3 = TrxC
h0 = sha256(input0)
h1 = sha256(input1)
h2 = sha256(input2)
h3 = sha256(input3)
h01 = sha256(h0 + h1)
h23 = sha256(h2 + h3)
h0123 = sha256(h01 + h23)

图4

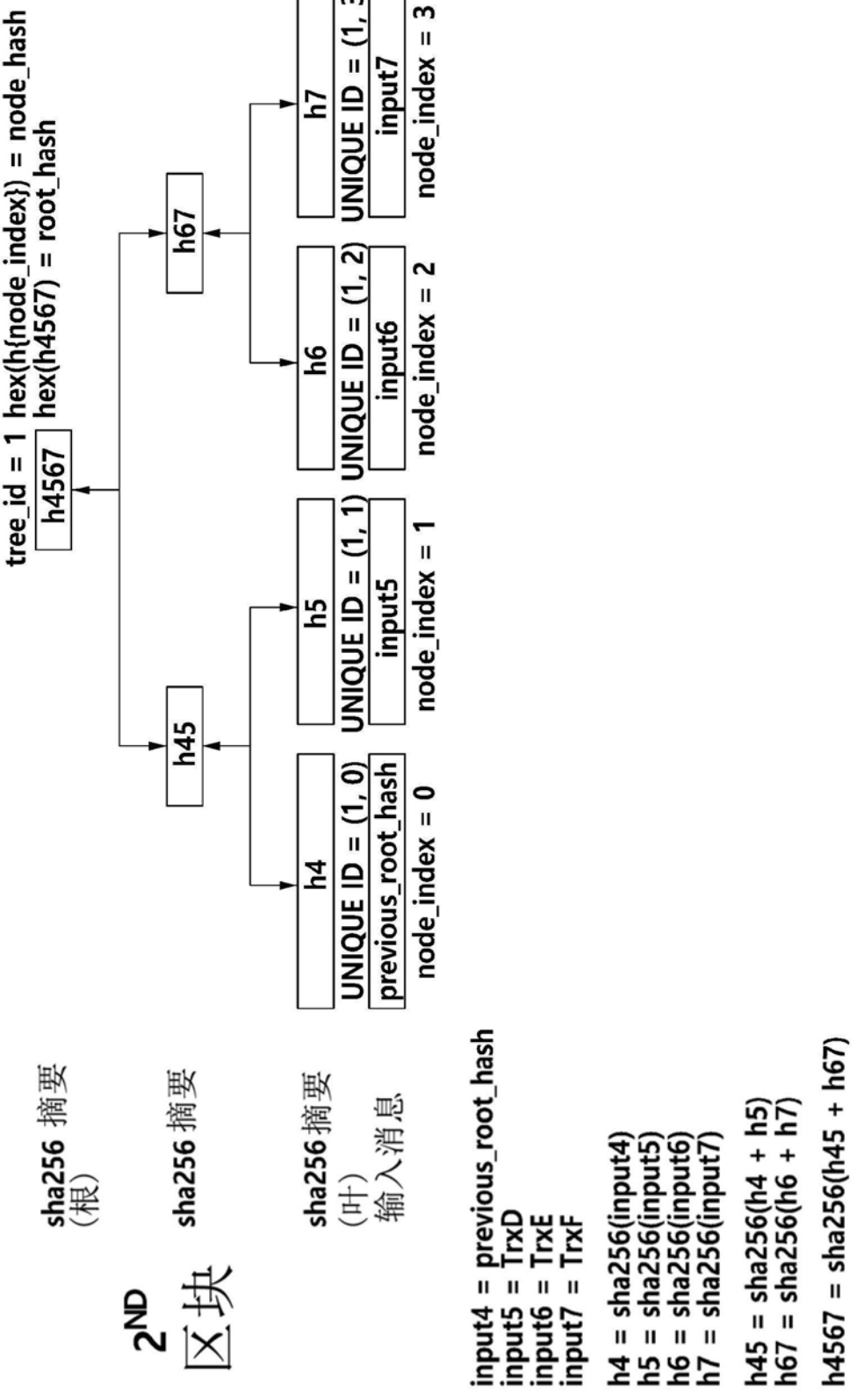
tree_id = 1 hex(h{node_index}) = node_hash
hex(h4567) = root_hash
h4567
h45
h67
h4
h5
h6
h7
UNIQUE ID = (1, 0)
UNIQUE ID = (1, 1)
UNIQUE ID = (1, 2)
UNIQUE ID = (1, 3)
previous_root_hash
input5
input6
input7
node_index = 0
node_index = 1
node_index = 2
node_index = 3
sha256 摘要
(根)
sha256 摘要
sha256 摘要
(叶)
输入消息
2ND
区块
input4 = previous_root_hash
input5 = TrxD
input6 = TrxE
input7 = TrxF
h4 = sha256(input4)
h5 = sha256(input5)
h6 = sha256(input6)
h7 = sha256(input7)
h45 = sha256(h4 + h5)
h67 = sha256(h6 + h7)
h4567 = sha256(h45 + h67)

图5

```
contract useCounter{
  int counter;
  function useCounter(int initNumber){
     counter = initNumber;
  }
  function decrease() constant returns (int){
     counter -= 1;
     return counter;
  }
}
```

图6

```
contract useCounter{
  int counter;
  function useCounter(){
     counter = 10;
  }
  function decrease() constant returns (int){
     counter -= 1;
     return counter;
  }
}
```

图7