(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 111034114 B
(45)授权公告日 2023.07.28

(21)申请号 201780093706.9
(22)申请日 2017.08.07
(65)同一申请的已公布的文献号
申请公布号 CN 111034114 A
(43)申请公布日 2020.04.17
(85)PCT国际申请进入国家阶段日
2020.02.06
(86)PCT国际申请的申请数据
PCT/US2017/045772 2017.08.07
(87)PCT国际申请的公布数据
WO2019/032089 EN 2019.02.14
(73)专利权人 维萨国际服务协会
地址 美国加利福尼亚州
(72)发明人 A·西拉 C·莱
(74)专利代理机构 上海专利商标事务所有限公司 31100
专利代理师 钱慰民 张鑫
(51)Int.Cl.
H04L 9/06(2006.01)
(56)对比文件
CN 106295401 A,2017.01.04
US 2017005804 A1,2017.01.05
US 2017213209 A1,2017.07.27
WO 2017127564 A1,2017.07.27
审查员 杨丽鲜

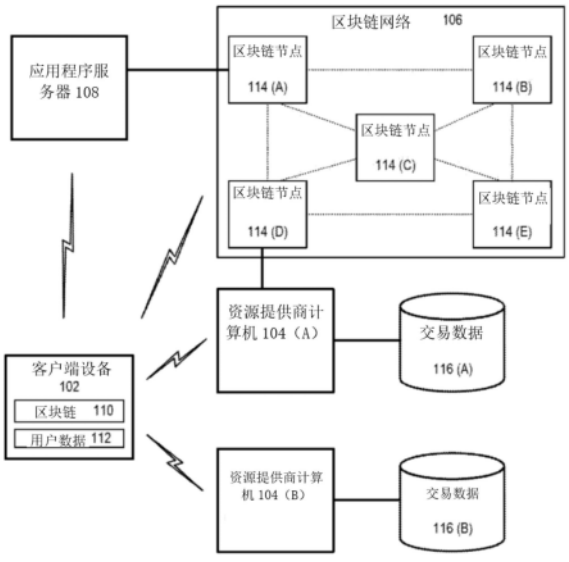
权利要求书2页 说明书17页 附图7页

(54)发明名称

具有记录安全性的区块链架构

(57)摘要

本文描述了一种系统，其中电子记录存储在分布式环境中。在该系统中，验证节点可以从接受节点接收交易记录。所述验证节点可以验证所述接受节点被授权参与区块链网络，识别与所述交易记录相关联的用户，并将所述交易记录附加到电子记录上。所述交易记录可以与通过以下方式形成的数字签名相关联：对多个数据元素进行散列处理，然后使用私有加密密钥对所散列的数据元素进行加密。



CN 111034114 B

1.一种用于改进区块链上的交易记录的安全性的方法,包括:

由验证节点从接受节点接收在所述接受节点与用户之间进行的交易的交易记录,所述交易记录包括至少与所述用户有关的信息和交易细节;

基于与所述用户有关的所述信息,识别与所述交易相关联的区块链;

将所述交易记录附加到所述区块链;

通过以下方式生成签名:

生成与所述用户有关的所述信息的至少一部分的第一散列;

生成所述交易细节的至少一部分的第二散列;

将所述第一散列和所述第二散列组合成文本字符串,其中组合所述第一散列和所述第二散列包括级联所述第一散列和所述第二散列;

将所述文本字符串进行散列处理以形成第三散列,所述第三散列是所述文本字符串的派生形式;以及

使用与所述验证节点相关联的私钥对所述文本字符串的所述派生形式进行签名,以形成所述签名;以及

将所述签名附到所述区块链内的所述交易记录上。

2.如权利要求1所述的方法,其中所述接受节点是由资源提供商操作的计算机。

3.如权利要求1所述的方法,其中所述私钥是RSA加密密钥。

4.一种验证节点服务器,包括:

一个或多个处理器;以及

存储器,所述存储器包括指令,所述指令当由所述一个或多个处理器执行时使得所述验证节点服务器:

从接受节点接收在所述接受节点和用户之间进行的交易的交易信息,所述交易信息包括至少用户信息和交易细节;

基于所述用户信息,识别与所述交易相关联的区块链;

至少部分地基于所述交易信息来生成交易记录;

将所述交易记录附加到所述区块链上;

通过以下方式生成签名:

生成所述用户信息的至少一部分的第一散列;

生成所述交易细节的至少一部分的第二散列;

将所述第一散列和所述第二散列组合成文本字符串,其中组合所述第一散列和所述第二散列包括级联所述第一散列和所述第二散列;

将所述文本字符串进行散列处理以形成第三散列,所述第三散列是所述文本字符串的派生形式;以及

使用与所述验证节点相关联的私钥对所述文本字符串的所述派生形式进行签名,以形成所述签名;以及

将所述签名附到所述区块链内的所述交易记录上。

5.如权利要求4所述的验证节点服务器,其中所述指令还使所述验证节点服务器在所述区块链网络内分发公钥。

6.如权利要求4所述的验证节点服务器,其中所述指令还使所述验证节点服务器在将

所述交易记录附加到所述区块链上之前，确定所述接受节点是否被授权参与所述区块链网络。

7.如权利要求4所述的验证节点服务器，其中所述用户信息的至少一部分的所述第一散列包括电子标识符。

8.如权利要求4所述的验证节点服务器，其中所述指令还使所述验证节点服务器将所述区块链分发到与所述用户相关联的客户端设备。

具有记录安全性的区块链架构

背景技术

[0001] 在资源提供商完成与用户的交易之前，通常希望资源提供商确定交易的风险级别。例如，银行机构可能希望评估与向特定个人或企业提供信贷额度相关的风险。在常规系统中，资源提供商可以咨询征信机构或其他实体，以确定每个用户的风险级别。

[0002] 但是，此类征信机构和其他实体可能仅构成单一信息来源。结果，从这样的实体检索数据可能是缓慢且繁重的。此外，由于人为错误或计算机故障，此类实体持有的数据可能会被破坏或错误。因此，需要解决这些问题的改进的系统和方法。

[0003] 本发明的实施方案单独地或共同地解决了这些和其他问题。

发明内容

[0004] 本公开的实施方案涉及一种系统，其中可以在分布式环境内针对用户生成电子记录(例如，分类账)。电子记录可以包括多个涉及用户的交易记录，其中每个交易记录都与资源提供商实体相关联，并由服务提供商使用该服务提供商的私钥进行签名。交易记录可以与用户相关联，并且可以在服务提供商接收到交易记录时将其附加到与该用户相关联的分类账中。在一些实施方案中，交易细节和/或用户信息可以被散列，以防止对个人细节的未授权访问。与交易和用户都相关的散列信息可以被组合，再次散列，然后使用私钥进行签名以形成签名，该签名可以用于验证分类账中交易细节和用户信息的真实性。该信息的真实性可以由希望向用户提供资源的资源提供商来验证。在一些实施方案中，资源提供商可以重新生成上述散列的和组合的数据。然后，用户可以使用与私钥相对应的公钥来验证签名。

[0005] 本发明的一个实施方案涉及一种方法，其包括：接收在接受节点和用户之间进行的交易的交易记录，该交易记录包括至少与用户有关的信息和交易细节；基于与用户有关的信息，识别与交易相关联的区块链；将交易记录附加到区块链；通过以下方式来生成签名：生成与用户有关的信息的至少一部分的第一散列；生成交易细节的至少一部分的第二散列；将第一散列和第二散列组合到文本字符串中；以及使用与验证节点相关联的私钥对文本字符串进行签名以形成签名，并将签名附到区块链内的交易记录上。加密密钥是RSA加密密钥。

[0006] 本发明的另一实施方案涉及一种包括一个或多个处理器和存储器的验证节点服务器。存储器包括指令，当指令由一个或多个处理器执行时，使验证节点服务器：接收关于在接受节点和用户之间进行的交易的交易信息，该交易信息包括至少用户信息和交易细节；以及识别与交易相关联的区块链；至少部分地基于交易信息生成交易记录；将交易记录附加到区块链；通过以下方式来生成签名：生成至少一部分用户信息的第一散列值；生成至少一部分交易细节的第二散列值；将第一散列值和第二散列值组合为文本字符串；以及使用与验证节点相关联的私钥，对文本字符串进行签名，以形成签名；并将签名附到区块链内的交易记录上。

[0007] 本发明的另一实施方案涉及一种资源提供商计算机，该资源提供商计算机包括一个或多个处理器以及包括指令的存储器，该指令在由一个或多个处理器执行时使该资源提

供商计算机接收完成该资源提供商计算机和用户之间的交易的请求，该请求包括至少与用户有关的信息；访问与用户相关联的用户区块链，该用户区块链由验证节点服务器生成，并包括多个交易记录；使用与用户有关的信息、包括在至少一个交易记录中的信息以及与验证节点服务器相关联的公钥来验证多个交易记录中的至少一个交易记录；在验证至少一个交易记录时，基于多个交易记录来确定交易的风险级别；并在确定交易的风险级别低于风险阈值级别后完成交易。

[0008] 本发明的这些和其他实施方案将在下文更详细地描述。

附图说明

[0009] 图1示出了根据至少一些实施方案的示例性系统的框图，在该示例性系统中，与用户相关联的电子记录可以被分发给资源提供商并由资源提供商验证；

[0010] 图2描绘了根据至少一些实施方案的示例性区块链节点服务器和示例性资源提供商计算机104的图；

[0011] 图3描绘了可以根据本公开的至少一些实施方案执行的过程的说明性示例。

[0012] 图4描绘了根据至少一些实施方案的用于生成签名的过程的说明性示例，该签名可以被附加到分类账内的交易记录以便能够对该交易记录进行验证；

[0013] 图5描绘了可以根据本公开的实施方案实现的示例电子记录；

[0014] 图6描绘了可以根据至少一些实施方案实现的所描述的系统的部件之间的交互的说明性示例；

[0015] 图7描绘了根据至少一些实施方案的用于在分布式环境内生成和维护电子记录的示例过程；以及

[0016] 图8描绘了根据至少一些实施方案的用于使用在分布式环境内维护的用户区块链来处理交易的示例过程。

具体实施方式

[0017] 在以下描述中，将描述各种实施方案。出于解释的目的，阐述特定配置和细节以便提供对实施方案的透彻理解。然而，所属领域的技术人员也应清楚，可在无所述特定细节的情况下实践实施方案。此外，可能省略或简化众所周知的特征以免使描述的实施方案模糊不清。

[0018] 在论述本发明的一些实施方案的细节之前，对一些术语的描述可有助于理解各种实施方案。

[0019] “应用程序服务器”可以是被配置为为客户端设备提供远程支持的任何计算设备。应用程序服务器可以与将被安装在客户端设备(例如，移动应用程序)上并且从客户端设备执行的一组计算机可执行指令相关联。应用程序服务器可以为客户端设备提供任何合适的服务和/或处理。例如，应用程序服务器可以代表客户端设备执行计算。在一些实施方案中，应用程序服务器可以保持一个或多个用户的账户。应用程序服务器还可以存储与客户端设备的操作相关的任何协议和/或用户偏好。

[0020] “区块链”可以是分布式数据库，该分布式数据库保持不断增长的记录列表，防止对该记录列表进行篡改和修订。区块链可以包括许多用户的许多交易记录区块。区块链中

的每个区块还可以包含时间戳和到前一个区块的链接。换句话讲，区块链中的交易记录可以作为包括在给定时间段内发生的许多交易的记录的一系列“区块”或永久文件被存储在电子记录中。在由适当的节点完成区块并且在该区块被证实之后，可以由该适当的节点将区块附加到区块链上。在本发明的实施方案中，可以分发区块链，并且可以在区块链网络中的每个节点处保持区块链的副本。区块链网络中的任何节点随后都可以使用区块链来验证交易。

[0021] “客户端设备”可以是能够与另一个电子设备(例如，应用程序服务器)建立通信会话并且能够从该设备传输/接收数据的任何电子设备。客户端设备可以包括下载和/或执行移动应用程序的能力。客户端设备可以包括移动通信设备以及个人计算机和瘦客户端设备。

[0022] “加密密钥”可以是被加密算法用来将纯文本转换为加密文本或将加密文本转换为纯文本的任何位串。加密密钥可以包括对称密钥和非对称密钥。加密密钥可以用于对交易进行签名和/或验证已签名的交易。例如，可以使用私有秘钥对加密货币交易进行签名。然后可以使用与该私有秘钥相对应的公共秘钥来验证已签名的交易。

[0023] “电子标识符”可以是用于识别实体(例如，人或设备)的任何合适的字符串或符号串。在一些实施方案中，电子标识符可以是通过散列可用于多个实体的一个或多个输入值而计算出的值。以此方式，电子标识符可以由具有前提条件信息的任何实体独立地生成。为了防止未经授权的一方访问电子记录，可以对电子标识符进行散列处理或加密。例如，电子标识符可以包括国家代码、客户姓名、出生日期以及社会保险号的最后四位数字的组合，例如SHA256(USA*JOHN SMITH*19700101*1234)。对此值进行散列可能会导致看似随机的字符串，例如444E982513BF546050C2D079FF5D65AB6E318E1AB5C1C。

[0024] “电子记录”可以是任何以电子方式存储的交易记录。例如，电子记录可以包括与电子标识符相关联的多个交易记录。在一些实施方案中，可以通过标识在分布式环境中记录的与特定电子标识符相关联的每个交易记录来编译电子记录。在一些实施方案中，电子记录可以包括由与电子标识符相关联的用户生成并且使用与之相关联的私有秘钥签名的部分。在一些实施方案中，电子记录可以是区块链的形式。

[0025] “分类账”可以是任何包含交易记录的电子记录。在一些实施方案中，分类账可以是由区块链网络生成的电子记录，使得当交易记录被附加到该分类账时，这些交易记录被链接到先前的交易记录并且使用私有秘钥进行签名。然后，可以由拥有交易记录信息和与私有秘钥相关联的公共秘钥的任何实体来验证分类账的真实性。

[0026] “移动通信设备”可以是具有与通信相关的主要功能的任何便携式电子设备。例如，移动通信设备可以是智能电话、个人数据助理(PDA)或任何其他合适的手持设备。移动通信设备可以被配置为输入加密货币地址并且显示任何接收的别名。在一些实施方案中，移动通信设备可以被配置为存储将要与加密货币地址和/或别名相关联的私有秘钥。

[0027] “私有秘钥”是一种由一方保密的加密密钥。私有秘钥可以用于对交易进行签名，使得可以使用区块链网络对所述交易进行验证。

[0028] “公钥”可以是分发给除持有对应的私有秘钥的一方以外的一些实体或对其可用的一种类型的加密密钥。在一些实施方案中，密钥可以是公开可用的，而在其他情况下，可以将其分发给网络中的节点，但是一般公众可能无法访问网络本身。可以使公共秘钥可用

于区块链网络的节点和/或资源提供商，使得与公共秘钥相关联的已签名交易可以由节点进行验证。

[0029] 术语“资源”通常是指可以使用或消耗的任何资产。例如，资源可以是计算机资源(例如，存储的数据或联网的计算机账户)，物理资源(例如，有形对象或物理位置)或其他电子资源或计算机之间的通信(例如，对应于用于执行交易的账户的通信信号)。资源的一些非限制性示例可以是商品或服务，物理建筑物，计算机账户或文件，或支付账户。在一些实施方案中，资源可以指金融产品，例如贷款或信贷额度。

[0030] “资源提供商”可以是可以提供诸如商品、服务、信息和/或访问的资源的实体。资源提供商的实例包含商家、访问设备、安全数据访问点等等。“商家”通常可以是参与交易并且可出售商品或服务或提供对商品或服务的访问的实体。

[0031] “服务器计算机”可以包括功能强大的计算机或计算机集群。举例来说，服务器计算机可以是大型主机、小型计算机集群或像单元一样工作的一组服务器。在一个实例中，服务器计算机可以是耦合到网络服务器的数据库服务器。服务器计算机可耦合到数据库，且可包含用于服务来自一个或多个客户端计算机的请求的任何硬件、软件、其他逻辑或前述内容的组合。服务器计算机可包括一个或多个计算设备，且可使用各种计算结构、布置和编译中的任一种来服务来自一个或多个客户端计算机的请求。

[0032] “交易记录”可以是在用户和另一实体之间进行的交易的任何指示。交易记录可以包括与所进行的交易相关的许多细节。例如，交易记录可以包括关于交易涉及的各方、进行的交易的类型、已经进行交易的金额或任何其他合适的信息的指示。

[0033] 术语“验证”及其派生形式可以指利用信息来确定基础主题在一组给定的情况下是否有效的过程。验证可以包括任何信息比较以确保某些数据或信息是正确的、有效的、准确的、合法的和/或信誉良好的。

[0034] 现在将描述本发明的一些实施方案的细节。

[0035] 图1示出了根据至少一些实施方案的示例性系统的框图，在该示例性系统中，与用户相关联的电子记录可以被分发给资源提供商并由资源提供商验证。在图1中，客户端设备102可以经由网络连接与一个或多个单独的实体进行通信。例如，客户端设备102可能能够与资源提供商计算机104，区块链网络106和/或应用程序服务器108建立通信。在一些实施方案中，系统可以包括多个资源提供商计算机104(每个都可以与不同的资源提供商实体相关联)和/或区块链网络106。在一些实施方案中，区块链网络可以是仅授权实体可以参与其中的联合区块链网络。可以代表服务提供商实体来运营区块链网络。

[0036] 根据本公开的实施方案，客户端设备102可以包括能够交互、存储和管理电子记录(例如，分类账)的任何合适的计算设备。客户端设备102可以包括至少处理器和存储器。客户端设备102的存储器可以包括至少电子记录(例如，分类账110)和用户数据112。存储器还可包括计算机可执行指令，这些计算机可执行指令使处理器执行根据本公开的实施方案的某些功能。例如，存储器可以包括移动应用程序，该移动应用程序使移动设备使用所存储的电子记录来发起交易。这可以涉及将分类账110和用户数据112提供给资源提供商计算机104。

[0037] 客户端设备102的存储器可以包括安全执行环境，诸如安全存储器(例如，在低功率设备中可用的基于智能卡的技术)。在一些实施方案中，安全存储器可以包括安全元件。

安全元件(SE)可以是防篡改平台(通常为单芯片安全微控制器),该防篡改平台能够根据一组很好标识的可信权威组提出的规则和安全要求来安全地托管应用程序及其机密和密码数据(例如,密钥管理)。客户端设备102接收到的敏感信息(例如,用户数据112)可以存储在安全存储器中。

[0038] 在一些实施方案中,客户端设备102还可以与应用程序服务器108建立连接,该应用程序服务器通过维护和管理与用户和/或客户端设备102相关联的电子记录来为客户端设备102提供后端支持。在一些实施方案中,在执行移动应用程序时,客户端设备102可以与应用程序服务器建立通信会话,在该会话中,应用程序服务器代表移动应用程序执行至少一些处理。在一些实施方案中,应用程序服务器108可以保持与客户端设备102和/或其用户相关联的账户。由应用程序服务器108保持的账户可以存储与用户相关的许多数据。例如,应用程序服务器108可以存储用户数据112,分类账110或任何其他合适的用户数据。应用程序服务器108可以在接收到来自移动应用程序的请求时,将其所维护的用户数据的至少一部分编译成要提供给客户端设备102的数据文件。例如,应用程序服务器108可以根据请求向客户端设备102上的移动应用程序提供分类账110和用户数据112的副本。在一些实施方案中,应用程序服务器108可以与区块链网络106进行通信并从其接收更新的信息。

[0039] 在一些实施方案中,客户端设备102可以包括通信接口,该通信接口被配置为用于在客户端设备102与另一电子设备(例如,资源提供商计算机104,应用程序服务器108和/或管理对网络的访问的无线路由器)之间进行通信。合适的通信接口的示例可以包括被配置为使用近场通信(NFC)或其他射频或无线通信协议(诸如蓝牙、蓝牙低功耗(BLE)、无线局域网(例如,WiFi)、iBeacon等)发送和接收通信的射频(RF)收发器。在一些实施方案中,通信接口可以包括红外通信设备。在一些实施方案中,该通信接口可以包括长距离和短距离通信装置两者。例如,通信接口可以包括被配置为连接至蜂窝网络以便能够与所描绘的架构的各种其他部件进行通信的天线。

[0040] 区块链网络106可以包括跨许多区块链节点114(A-E)实现的分布式环境,每个区块链节点表示计算系统或部件。关于图2更详细地描述了可以根据各种实施方案实现的区块链节点服务器114的示例。可以将区块链的副本(电子记录的记录)分发给区块链网络106中的每个区块链节点114。在一些实施方案中,至少一些区块链节点114可以各自由服务提供商实体或资源提供商实体中的至少一者所有和/或操作。在一些实施方案中,区块链网络106可以包括由实体操作的许多计算设备,这些实体中的每个实体属于特定的组或已经获得特定证书。在一些实施方案中,资源提供商计算机104,客户端设备102或应用程序服务器108中的至少一个可以是区块链节点114。另外,一个或多个区块链节点114可以是验证节点,并且多个区块链节点114可以是接受节点。验证节点可以是由运营区块链网络106的服务提供商运营的区块链节点114。在一些实施方案中,仅验证节点可以使用与服务提供商相关联的私钥来对交易记录进行签名。接受节点可以是由参与区块链网络106的资源提供商计算机或客户端设备操作的区块链节点114。

[0041] 根据至少一些实施方案,区块链网络106可以包括联合的和/或基于权限的环境。例如,为了参与或使用区块链网络106,可能需要对实体进行证实或以其他方式认证。例如,区块链网络106可以要求每个实体遵循信任服务管理(TSM)策略和/或规则。在一些示例中,基于实体的类型,不同实体可能要遵循不同的策略。例如,与银行机构相关联的服务器可能

会自动被信任，而与个人相关联的服务器可能需要从银行机构接收证书。在这些示例中，仅可信实体可以访问或参与区块链网络106。

[0042] 在一些实施方案中，由区块链网络106保持的记录数据可以被存储，使得记录数据不容易与特定用户或账户持有者相关联。例如，记录数据可以包括许多资源定位符地址，这些资源定位符地址引用用户数据而不指示用户。在一些实施方案中，区块链网络106可以将与每个资源定位器地址有关的用户的记录存储在单独的数据存储中(例如，作为单独的分类账110)。

[0043] 资源提供商计算机104可以包括能够执行本文描述的操作的任何合适的计算设备。关于图2更详细地描述了可以根据各种实施方案实现的资源提供商计算机104的示例。如关于图2所描述的，资源提供商计算机104可以提供对一个或多个资源的访问。在一些实施方案中，每个资源提供商计算机104(A-B)都可以维护包括交易数据116(A-B)的相应数据库。交易数据116可以包括在资源提供商计算机104和许多用户之间进行的交易的记录。

[0044] 在一些实施方案中，资源提供商计算机104可以被配置为接收信息(诸如电子记录的指示)，执行对电子记录的验证以及基于该信息来确定用户的信用状态。在一些实施方案中，可以从客户端设备102(或代表客户端设备102，从应用程序服务器108)接收电子记录。在一些实施方案中，客户端设备102可以向电子记录所位于的资源提供商计算机104发送位置或地址。然后，资源提供商计算机104可以从区块链网络106请求电子记录或其他与账户有关的信息。例如，资源提供商计算机104可以在从客户端设备102接收到电子记录之后，验证(例如，通过使用服务提供商实体的公钥)电子记录中的服务提供商实体的签名，并基于电子记录中的信息来确定与电子记录相关联的用户的信用状态。

[0045] 在一些实施方案中，资源提供商计算机104也可以是能够访问区块链网络106并参与区块链网络的操作的区块链节点114。在一些实施方案中，资源提供商计算机104可能没有访问区块链网络106的权限，但是可以被提供有可以用于验证与区块链网络106相关联的电子记录的公钥。

[0046] 通过图示在本文描述的系统的各个部件之间的交互，考虑用户首先与资源提供商104(A)进行交易的场景。为了该场景的目的，假定资源提供商104(A)有权访问由第三方服务提供商(即，与资源提供商计算机104不存在附属关系的服务提供商)运营的区块链网络106。在这种情况下，资源提供商计算机104可以在其维护的交易数据数据库116中记录与交易有关的细节。另外，资源提供商计算机104将交易细节(包括交易细节以及用户的细节)发送到区块链网络106。

[0047] 在从资源提供商计算机104接收到交易细节之后，区块链网络106验证资源提供商计算机104被认证和/或被授权参与所描述的系统。然后，区块链网络106根据交易细节生成交易记录，然后对其进行签名(使用与区块链网络106相关联的私钥)，并将其附加到与用户相关联的分类账中。在一些实施方案中，可以将更新的分类账发送到与该用户相关联的客户端设备102(例如，通过推送通知)。在一些实施方案中，可以向客户端设备102授予对分类账存储位置的访问权。

[0048] 继续以上情形，用户可以选择与资源提供商计算机104(B)进行第二次交易，其中用户可能需要表现出信誉。资源提供商计算机104(B)可能能访问或可能不能访问区块链网络106，但是应该能访问与区块链网络106相关联的公钥(例如，公钥可以存储在本地)。为了

表现出信誉，用户可以将分类账与相关数据(例如，用户数据和/或交易记录)一起从客户端设备发送到资源提供商计算机104(B)。然后，资源提供商计算机104(B)能够使用公钥来验证电子记录的真实性。一旦被验证，资源提供商计算机104(B)可以基于所提供的分类账来确定关于用户的信誉，该分类账包括用户的过去交易记录的指示。在资源提供商计算机104(B)不能访问区块链网络106的实施方案中(例如，在对互联网的访问受到限制的情况下)，这允许资源提供商计算机104(B)在本地进行信用检查，同时确保信用报告数据的准确性。通过进一步阐述该说明性情形，资源提供商计算机104(B)可以稍后将交易细节提供给区块链网络(例如，当恢复互联网访问时)，其随后可以基于交易细节来更新用户的分类账。

[0049] 为了简化说明，图1中示出一定数量的部件。然而，应理解，本发明的实施方案可包含多于一个每种部件。另外，本发明的一些实施方案可包含比图1中所示的所有部件少或多的部件。此外，图1中的部件可以经由任何合适的通信介质(包括互联网)使用任何合适的通信策略来进行通信。

[0050] 图2描绘了根据至少一些实施方案的示例性区块链节点服务器114和示例性资源提供商计算机104的图。验证节点服务器200可以是图1的示例区块链节点服务器114。资源提供商计算机104可以是图1的示例资源提供商计算机104。

[0051] 验证节点服务器200可以是能够执行以下操作的任何类型的计算设备，其能够从资源提供商计算机104接收交易记录，更新与用户相关联的分类账以包括来自交易记录的信息，使用私钥对分类账进行签名以及将分类账分发到与用户相关联的客户端设备。在至少一些实施方案中，资源提供商计算机104可以包括至少一个存储器202和一个或多个处理单元(或一个或多个处理器)204。处理器204可以在硬件、计算机可执行指令、固件或其组合中适当地实现。处理器204的计算机可执行指令或固件实施方案可以包括以任何合适的编程语言编写的用于执行所描述的各种功能的计算机可执行指令或机器可执行指令。

[0052] 存储器202或本文所描述的任何其他存储器可以存储在处理器上可加载和可执行的程序指令，以及在这些程序指令的执行期间生成的数据。存储器可以是易失性的(诸如随机存取存储器(RAM))和/或非易失性的(诸如只读存储器(ROM)、闪存存储器等)。验证节点服务器200还可以包括附加存储设备206，诸如可移动存储设备或不可移动存储设备，包括但不限于磁存储设备、固态存储设备、光盘和/或磁带存储设备。盘驱动器及其相关联的计算机可读介质可以为验证节点服务器200提供计算机可读指令、数据结构、程序模块和其他数据的非易失性存储。在一些实施方案中，存储器202可以包括多种不同类型的存储器，诸如静态随机存取存储器(SRAM)、动态随机存取存储器(DRAM)或ROM。

[0053] 更详细地转向存储器202的内容，存储器202可以包括操作系统208和用于实现本文所公开的特征的一个或多个应用程序或服务，所述一个或多个应用程序或服务包括至少用于生成和管理与用户相关联的电子记录的模块(记录管理模块210)。存储器202还可以包括提供与用户的交易历史相关联的数据的分类账数据212和提供与用户和/或账户相关联的数据的用户数据214。

[0054] 在一些实施方案中，记录管理模块210可以与处理器204结合，被配置为接收来自资源提供商的交易记录，从那些交易记录生成用户区块链，并且将用户区块链发送到与用户相关联的客户端设备。在一些实施方案中，记录管理模块210可以在接收到交易细节时，生成交易信息的第一散列和用户信息的第二散列。然后可以将两个散列组合(例如，级联)。

在一些实施方案中，组合信息或其派生形式(例如，组合信息的散列)可用于生成用户/交易消息摘要值。然后，验证节点服务器200使用与验证节点服务器200相关联的私钥对用户/交易消息摘要值进行签名。在整个公开中，该签名信息可以被称为签名。签名一旦生成，就可以附加到用户区块链内的交易记录中。然后，另一个实体可以使用相应的公钥来验证分类账内单个交易记录的合法性。一旦分类账已被更新以包括新的交易记录信息，则记录管理模块210可以使该分类账对与用户相关联的客户端设备可用。

[0055] 在一些实施方案中，资源提供商计算机104可以是能够执行以下操作的任何类型的计算设备：其能够从客户端设备接收电子记录，验证验证节点服务器200已经对电子记录进行了签名以及基于电子记录，确定是否准予客户端设备的用户对资源进行访问。在至少一些实施方案中，资源提供商计算机104可以包括至少一个存储器220和一个或多个处理单元(或一个或多个处理器)222。与验证节点服务器200相似，资源提供商计算机104也可以包括附加存储器206。

[0056] 更详细地转向存储器220的内容，存储器220可以包括操作系统224和用于实现本文公开的特征的一个或多个应用程序或服务，应用程序或服务包括至少用于验证电子记录的真实性的模块(验证模块226)和/或用于基于电子记录来确定是否授权交易的模块(授权模块228)。存储器220还可以包括交易数据230，交易数据提供与资源提供商计算机104进行的历史交易相关联的数据。

[0057] 在一些实施方案中，验证模块226可以与处理器222一起被配置为验证从客户端设备接收到的分类账的一个或多个交易记录的真实性。在一些实施方案中，资源提供商计算机104可以维护与验证节点服务器200相关联的公钥。为了验证交易记录的真实性，验证模块226可以通过使用与验证节点服务器200的记录管理模块210执行的过程类似的过程来独立地生成用于签名的用户/交易消息摘要值。然后，可以由验证模块226使用与验证节点服务器200相关联的公钥来验证签名。验证模块226可以将独立生成的用户/交易消息摘要值与通过使用验证算法将公钥应用于签名而获得的值进行比较。匹配表示交易记录是合法的。

[0058] 在一些实施方案中，授权模块228可以与处理器222一起被配置为基于所提供的分类账内的交易记录来确定是否授权交易。在一些实施方案中，交易记录可以正面或负面地反映用户的信誉。例如，交易记录可以指出用户未能支付账单或用户按时支付了账单。授权模块228可以使用特定于资源提供商计算机104的算法，以基于分类账中的交易记录来计算用户的信誉。在某些情况下，每个资源提供商计算机104都可以将不同的权重分配给特定的交易记录。

[0059] 验证节点服务器200和/或资源提供商计算机104也可以包含通信接口216，这些通信接口使相应的服务器能够与存储的数据库，另一计算设备或服务器，一个或多个远程设备，其他应用程序服务器，和/或任何其他合适的电子设备进行通信。在一些实施方案中，通信接口216可以使得服务器能够与网络上(例如，专用网络上)的其他电子设备进行通信。相应的服务器104还可以包括一个或多个输入/输出(I/O)设备和/或端口218，诸如用于实现与键盘、鼠标、笔、语音输入设备、触摸输入设备、显示器、扬声器、打印机等的连接。

[0060] 图3描绘了可以根据本公开的至少一些实施方案执行的过程300的说明性示例。在图3中，客户端设备302可以与一个或多个资源提供商计算机(例如，资源提供商计算机304

和/或资源提供商计算机306)进行通信。每个设备都可以与具有多个区块链节点服务器310的区块链网络308进行通信。在一些实施方案中,资源提供商计算机304和/或306中的至少一些可以是区块链节点服务器308。

[0061] 通过非限制性说明,资源提供商计算机304和资源提供商计算机306中的每一个都可以是由资源提供商实体(例如,商人、银行机构等)操作的计算设备。在该示例中,用户可以在第一时间点开通要由区块链网络308维护的账户,并且随后可以被提供有与该用户相关联的电子记录。在注册过程中,用户可以提供客户端设备302的标识符(例如,电话号码、安全元件标识符、IMEI号码、SIM卡号码等),然后标识符与该用户的账户相关联。在一些实施方案中,即使一个用户在区块链网络308上没有账户,区块链网络308也可以获取该用户的交易记录。例如,多个资源提供商计算机304可以连续地向区块链网络308报告它们已经进行的交易。区块链网络308可以以每个唯一用户的用户区块链形式维护分类账,其中包括与该用户有关的每个交易记录。在用户未在区块链网络308上注册账户的实施方案中,资源提供商计算机304或306可从区块链网络308获得与用户相关联的分类账。这可以使资源提供商计算机能够获得对有关用户进行的任何交易的信息的访问,从而允许该实体更好地分析与用户相关联的风险。

[0062] 在过程300的步骤1,客户端设备302可以将分类账发送到资源提供商计算机304,以便获得对交易的批准。在一些实施方案中,客户端设备302可以向资源提供商计算机304提供用户信息(例如,电子标识符)以发起交易。在一些实施方案中,资源提供商计算机304可以根据客户端设备提供的请求中的用户特定的信息独立地生成电子标识符。在某些情况下,可以通过直接无线通信信道将分类账提供给资源提供商计算机304。例如,用户可以接近销售点(POS)终端并请求以信贷方式购买商品或服务。为了证明信誉,用户可以使客户端设备302将分类账发送到与资源提供商计算机304相关联的POS终端,然后,资源提供商计算机可以验证分类账并确定用户的信誉。在一些实施方案中,这可以涉及用户启动移动应用程序和/或在客户端设备302上登录到账户。

[0063] 在步骤2,资源提供商计算机304可以将进行的交易的细节报告给区块链节点服务器308。例如,资源提供商计算机304可以向验证节点服务器310报告任何影响信用的事件(例如,资源提供商计算机304是否授权交易)。在一些实施方案中,资源提供商计算机304可以存储用户的信息,并且可以在交易之后继续报告影响信用的事件。例如,资源提供商计算机304可以向验证节点服务器310报告用户是否已经按时支付了他或她的账单,未按时支付他或她的账单,或者还没有支付他或她的账单。当进行了付款或未进行付款时,该操作可以重复多次。在一些实施方案中,过程300不需要在步骤1开始。例如,在某些情况下,验证节点服务器310可以从多个资源提供商计算机304和306获得交易信息,而无需来自客户端设备302或用户的任何交互。

[0064] 在步骤3,区块链节点服务器308可以更新与用户相关联的分类账(诸如用户区块链),以包括由资源提供商计算机304向其提供的交易信息。在一些实施方案中,区块链节点服务器308可以首先验证资源提供商计算机304被授权报告交易记录。例如,区块链节点服务器308可以确定资源提供商计算机304是可信实体。在一些情况下,区块链节点服务器308可以具有与可信资源提供商计算机相关联的标识符的数据库。基于先前的注册过程和/或先前的交互,它们可以被信任。在一些实施方案中,区块链节点服务器308可以确定与特定

实体相关联的信任级别。在这些实施方案中，验证节点服务器310可以不管资源提供商计算机304是否是可信实体而处理交易记录，但是可以在交易记录中包括分配给资源提供商计算机304的信任级别的指示。在一些实施方案中，验证节点服务器310还可以在记录交易信息之前确定该交易信息是否是重复的(例如，已经包括在用户分类账中)。

[0065] 在确定可以记录由资源提供商计算机304提供的交易信息时(例如，资源提供商计算机304被授权并且交易信息不是重复的)，验证节点服务器310可以识别要更新的适当分类账。在一些实施方案中，用户分类账可以与相应的电子标识符相关联地存储，使得个人信息不能被映射到特定的交易记录。在一些实施方案中，验证节点服务器310可以根据资源提供商计算机304提供的用户信息独立地生成电子标识符。在一些实施方案中，资源提供商计算机304可以提供电子标识符。分类账可能包括许多与用户的财务状况有关的文件和/或交易细节。例如，分类账可以包括对与用户相关联的资产的引用(例如，房契等)，该用户的未清信贷额度和/或与该用户的财务状况有关的任何其他合适的信息。

[0066] 在步骤4，可以给与用户相关联的客户端设备302访问更新的分类账的权限。在一些实施方案中，可以向客户端设备302提供更新的分类账的副本。在一些实施方案中，可以向客户端设备302提供更新分类账的位置或到更新分类账的链接。分类账可以是数据文件，并且可以供安装在客户端设备302上并从其执行的移动应用程序使用。在一些实施方案中，分类账可以被加密以确保未授权用户不会获得对分类账中交易记录信息的访问。

[0067] 在步骤5，客户端设备302可以将分类账发送到第二资源提供商计算机306，以便获得对第二交易的批准。如在步骤1中，客户端设备302可以向资源提供商计算机306提供用户信息(例如，电子标识符)以发起交易，或者资源提供商计算机306可以根据由客户端设备提供的请求中的用户特定的信息独立地生成电子标识符。在某些情况下，可以通过直接无线通信信道将分类账提供给资源提供商计算机306。在其他实施方案中，客户端设备302可以提供信息(例如URL)，其可以向资源提供商计算机306提供对分类账的访问。

[0068] 应当注意，在某些情况下，资源提供商计算机306可以从除客户端设备302之外的源访问(例如，接收)分类账。例如，在经由客户端设备302接收到进行交易的请求时，资源提供商计算机304/306可以联系区块链网络308以获得与用户相关联的分类账。在一些实施方案中，资源提供商计算机304和306中的一个或多个也可以是区块链节点服务器310，其维护分布式分类账的副本。在这些实施方案中，可以使用与用户相关联的电子标识符来识别适当的分类账。在某些情况下，电子标识符可以由资源提供商计算机使用提供的用户信息独立生成。例如，在接收到包括与用户有关的信息的执行交易的请求时，资源提供商可以根据所提供的信息生成电子记录，识别适当的用户区块链，验证用户区块链内的交易记录，并基于用户区块链中的交易信息，确定是否批准或拒绝交易。

[0069] 为了从区块链网络308请求分类账，可能需要资源提供商计算机306呈现用户的电子标识符。例如，资源提供商计算机306可以组合与用户进行交易的任何实体将可以访问的许多信息字段。在一些实施方案中，资源提供商计算机306然后可以进一步将组合的数据(例如，通过对该数据进行散列处理)处理成电子标识符。例如，第一实体服务器可以通过组合诸如国家代码、客户姓名、生日和社会保险号的后四位数字之类的用户特定信息来创建电子标识符，诸如“SHA256(USA*JOHN SMITH*19700101*1234)”。在此示例中，第一实体服务器随后可以使用公开可用的散列函数对该电子标识符进行散列处理，以获取电子标识符的

散列，例如字符串“444E982513BF546050C2D079FF5D65AB6E318E1AB5C1C0BC5F810D35348745FBA12A”。可以识别用户的分类账并将其提供给资源提供商计算机306。以这种方式，可以将分类账提供给拥有某些用户特定的信息的任何实体，同时对该用户特定的信息进行散列处理，以防止未经授权的第三方获取该用户特定的信息。此外，也无法从散列值确定电子标识符。这意味着验证节点服务器310可以要求用户数据的任何请求者提供电子标识符，以证明请求者有权访问用户数据。由于未授权实体将不能访问电子标识符，因此这防止了未授权实体偶然发现交易记录，并且简单地向验证节点服务器310请求敏感的用户信息。另外，简单地提供随机生成的电子标识符将是徒劳的，因为请求者将无法将获得的任何信息映射到特定用户。

[0070] 通过说明性示例，考虑以下情形。在一些实施方案中，资源提供商实体中的至少一个(例如，资源提供商计算机304和/或资源提供商计算机306)可以维护物理位置。例如，资源提供商可以包括运营分支机构的银行机构。在该示例中，操作客户端设备302的用户可以输入分支机构地址以便建立账户，请求贷款或执行任何其他合适的操作。用户可以独立地向银行机构提供许多个个人和/或财务细节，这些细节随后可以由银行机构服务器存储在关于用户的记录数据中。另外，银行机构可以(根据用户的个人详细信息)生成与用户相关联的电子标识符。在验证用户的真实性后，银行机构可以从用户的客户端设备302接收分类账，或者从区块链网络308请求分类账。

[0071] 在步骤6，资源提供商计算机306可以验证分类账内一个或多个交易记录的真实性，并确定是否批准交易。在一些实施方案中，资源提供商计算机306可以验证分类账的某些部分(例如，与电子记录相关联的单个交易记录)。为此，资源提供商计算机306可以识别对与电子记录相关联的交易记录进行签名的区块链网络308，识别该区块链网络的公钥(例如，来自公钥的存储库)，独立地生成用户/交易消息摘要，并使用识别出的公钥来验证交易记录是否是使用区块链网络的私钥进行签名的。这可能涉及使用公钥来验证交易记录，以便验证交易记录的特定格式或内容。例如，这可能涉及将生成的用户/交易消息摘要与从交易记录中的签名获得的值进行比较。在一些实施方案中，资源提供商计算机306可以验证分类账中的每个交易记录。在一些实施方案中，资源提供商计算机306可以仅验证分类账中的交易记录的一部分。例如，资源提供商计算机306可以从分类账中随机选择交易记录以进行验证。

[0072] 在步骤7，资源提供商计算机306可以用关于交易是否被批准的指示来响应客户端设备302。为了确定是否批准交易，资源提供商计算机306可以识别与分类账中的每个交易记录相关联的不同实体，并确定将与那些实体中的每个实体相关联的信任值。然后，资源提供商计算机306可以识别与超过信任阈值的信任值相关联的每个实体，从其中获得用户数据。因为资源提供商计算机306被提供有包括所有相关交易记录的分类账，所以资源提供商计算机306能够使用专有算法来进行信誉评估。专有算法可以将不同权重分配给与每个交易记录相关联的因素。例如，资源提供商计算机306可以将更大的权重分配给涉及与其自身相似的资源提供商的交易记录。在第二示例中，如果客户端设备302的用户与许多不同的交易记录相关联，这些交易记录涉及两个非常大的，众所周知的且可信赖的银行，以及两个不是很众所周知的较小的商家，则银行的信任值可以被确定为高于小商家的信任值，因为银行是众所周知的，并且受到严格的政府监管，而小商家则不然。在这种情况下，资源提供商

计算机306可以仅基于与银行相关联的交易记录来确定是否批准交易。

[0073] 在步骤8,资源提供商计算机306可以将进行的交易的细节报告给区块链节点服务器308。然后可以重复步骤3和4,以便向客户端设备302提供包括最新交易数据的更新分类账。应当注意,如虚线所示,资源提供商计算机306可以是或可以不是区块链网络308的参与者。在一些实施方案中,资源提供商计算机306甚至不需要有网络连接。只要资源提供商计算机306可以访问与区块链网络308相关联的公钥,资源提供商计算机306就能验证分类账的真实性,并且可以在不进行常规信用检查的情况下进行信誉确定。

[0074] 图4描绘了根据至少一些实施方案的用于生成签名的过程400的说明性示例,该签名可以被附加到分类账内的交易记录以便能够对该交易记录进行验证。如图2所描绘的,过程400可以由验证节点服务器200生成。

[0075] 在一些实施方案中,可以向验证节点服务器200提供用户信息402。在接收到用户信息402时,验证节点服务器200可以识别将被组合为文本字符串的用户信息的特定字段的值。用户信息402可以包括任何用户特定的信息。在一些实施方案中,文本字符串可以包括对用户进行信用检查的任何实体将可访问的信息的组合。在一个说明性示例中,验证节点服务器200可以将国家代码、客户姓名、生日和社会保险号的后四位组合为文本字符串。然后,可以在404对该文本字符串进行散列算法处理,以获得电子标识符406。

[0076] 在一些实施方案中,还可以向验证节点服务器200提供交易信息408。在接收到交易时,验证节点服务器200可以识别将被组合为文本字符串的交易信息408的特定字段的值。在一个说明性示例中,验证节点服务器200可以将资源提供商ID、交易金额和交易日期组合成文本字符串。然后,可以在410对该文本字符串进行散列算法处理,以获得交易信息消息摘要412。

[0077] 在414,区块链节点服务器可以将电子标识符406和交易信息消息摘要412组合成单个文本字符串。在一些实施方案中,可以在级联过程中组合信息。例如,在一些实施方案中,两个文本字符串(电子标识符406和交易信息消息摘要412)中的每一个都可以被转换为数字字符串,然后可以将两个数字字符串相加以形成第三字符串。在一些实施方案中,可以对该第三字符串执行散列算法416以生成用户/交易消息摘要418。交易消息摘要418可以是第三字符串的派生形式,第三字符串可以是文本字符串。

[0078] 一旦已经生成了用户/交易消息摘要418,区块链节点服务器就可以在420处对用户/交易消息摘要418进行签名,以便生成签名422。为了对用户/交易消息摘要418进行“签名”,区块链节点服务器可以使用一种或多种加密算法,以及与区块链网络相关联的私钥。然后,可以将签名附加到交易记录,然后,将交易记录添加到用户区块链。然后,资源提供商可以使用签名以及用户信息和交易记录中的信息来验证用户记录中交易记录的真实性。可以重复该过程以为用户区块链内的每个交易记录生成签名。

[0079] 为了验证使用上述过程生成的签名,资源提供商可以以上述方式(使用提供的用户信息和交易记录中的交易信息)独立生成用户/交易消息摘要418。然后,资源提供商可以通过使用一种或多种验证算法以及与区块链网络相关联的公钥来验证签名。然后,将独立生成的用户/交易消息摘要418与使用公钥、签名和验证算法获得的值进行比较,并且资源提供商计算机确定两个值是否匹配。匹配表示签名已通过验证。

[0080] 使用图4所示的数字签名过程具有许多优点。首先,交易和用户数据可以经受至少

三个散列处理，这为基础信息提供了更大的保护。此外，由用户信息402和交易信息412提供的数据是唯一的，使得所产生的消息摘要418对于该特定交易是唯一的并且是不可更改的。

[0081] 图5描绘了可以根据本公开的实施方案实现的示例电子记录。在图5中，电子记录，特别是用户区块链502，可以包括跨区块链网络分布的与特定用户相关的交易记录504的记录。在一些实施方案中，用户区块链502可以包括这样的区块链，其中在“区块”中处理与各种电子标识符相关的许多交易记录，然后将所述许多交易记录的记录分发给区块链网络的多个节点。

[0082] 如上所述，许多交易记录504可以与用户区块链502相关联。在一些实施方案中，用户区块链仅包含该用户的交易记录，而没有其他用户的交易记录。用户区块链502可以包括用户信息506，其可以被格式化为电子标识符。在一些实施方案中，可以针对用户生成电子标识符，该用户可以是特定的个人、设备或实体。在一些实施方案中，可以使用经由客户端设备提供的或在用户注册期间提供的用户信息来生成电子标识符。在一些实施方案中，电子标识符可以由区块链节点服务器基于提供的关于该用户的信息来生成，区块链节点服务器接收到与该用户有关的交易记录。可以使用与用户相关的信息根据指定的格式来生成电子标识符。

[0083] 当个人、设备或实体与各种实体进行交易时，与这些实体相关联的服务器508可以生成交易记录并将它们发送到区块链网络以附加到用户区块链502。在一些实施方案中，附加到用户区块链502的每个交易记录都可以包括签名510，该签名可以用于验证交易记录的真实性。签名510可以是根据图4中描绘的过程400生成的签名的示例。交易记录504还可以包括交易数据512。在一些实施方案中，包括在交易记录504中的交易数据512可以包括与所进行的交易，进行交易的实体相关的信息或任何其他合适的信息。

[0084] 当与用户区块链502相关联的个人、设备或实体与各种其他实体进行交易时，与这些实体相关联的其他服务器514可以生成其他交易记录，这些记录随后被提供给区块链网络并与用户区块链502相关联。每个交易记录都由区块链网络的验证节点进行签名并附加到用户区块链502。以此方式，可以生成用户区块链502以包括在个人、设备或实体与各种其他实体之间进行的许多交易。用户区块链502可以用于评估个人、设备或实体的信用等级、交易历史、凭证或任何其他合适的报告。

[0085] 图6描绘了可以根据至少一些实施方案实现的所描述的系统的部件之间的交互的说明性示例。在图6中，区块链网络602被描绘为包括多个节点。区块链网络602的节点可以包括至少一个验证节点604和多个接受节点。在一些实施方案中，区块链网络602的接受节点还可以包括由参与区块链网络602的资源提供商运营的服务器606。另外，区块链网络602的接受节点还可包括与参与区块链网络602的用户相关联的客户端设备608。在一些实施方案中，区块链网络602的验证节点604可以由与运营区块链网络602的接受节点的资源提供商实体和/或用户分开的服务提供商实体拥有和/或运营。

[0086] 在一些实施方案中，可以在区块链网络602的两个节点之间进行交易。在一个说明性示例中，资源提供商服务器606可以由信用卡发行商运营，并且客户端设备608(由用户操作)可以用于在步骤1中对由信用卡发行商维护的账户进行信用卡支付。在该示例中，资源提供商服务器606可以将交易记录在数据库中，并基于该交易来更新相关账户的状态。另外，信用卡发行商可以在步骤2将包括交易细节的交易记录发送到验证节点604。应该注意

的是，尽管图6将交易描述为从客户端设备608发起的，但是，在一些实施方案中，交易可以是由资源提供商服务器606本身发起的。例如，用户可以在自动支付系统中进行注册，在该系统中，定期自动进行支付。

[0087] 一旦验证节点604已经从资源提供商服务器606接收到交易记录，验证节点604就可以将交易记录附加到与账户相关联的用户区块链610。然后，验证节点604可以使用仅对验证节点604可用的私钥来对用户区块链610的交易记录进行签名。在步骤3，可以将更新的用户区块链分发到区块链网络602的每个验证节点604和接受节点，以包括至少每个资源提供商服务器606。在一些实施方案中，可以仅将用户区块链发送到与为其维护了用户区块链610的用户相关联的那些客户端设备608。

[0088] 用户区块链610可以包括与针对特定用户进行的多个交易有关的信息，并且可以被分布到区块链网络的每个验证节点604和至少一部分接受节点。在一些实施方案中，当用户向维护区块链网络602的接受节点的资源提供商请求资源(例如，服务或商品)时，与该资源提供商相关联的资源提供商计算机606可以查询存储库以识别与用户相关联的用户区块链610。一旦找到，资源提供商计算机606就可以验证用户区块链610的真实性。在验证用户区块链610之后，资源提供商计算机606就可以基于用户区块链来确定与用户相关联的风险级别。例如，资源提供商计算机606可以基于多个因素来将加权值分配给用户区块链610中的每个交易记录。在该示例中，资源提供商计算机610然后可以通过对加权值求和来估计风险级别。在一些实施方案中，资源提供商计算机606可以仅在确定风险级别低于预定阈值时才授权交易。

[0089] 图7描绘了根据至少一些实施方案的用于在分布式环境内生成和维护电子记录的示例过程。本文所描述的任何过程中的任一个的一些或全部(或变型和/或其组合)可以在配置有可执行指令的一个或多个计算机系统的控制下执行，并且其可以被实现为代码(例如，可执行指令、一个或多个计算机程序或一个或多个应用)。根据至少一个实施方案，图7的过程700可以由至少一个如图2所描绘的验证节点服务器来执行。验证节点服务器可以是区块链网络的节点。代码可以存储在计算机可读存储介质上，例如以包括可由一个或多个处理器执行的多个指令的计算机程序的形式。计算机可读存储介质可以是非瞬态的。

[0090] 过程700可以开始于702，此时从接受节点(例如，资源提供商计算机)接收到交易记录。在一些实施方案中，验证节点服务器可以首先确定接受节点是否被授权参与区块链网络。例如，验证节点服务器可以确定接受节点是否是可信实体(例如，经认证的)。在确定接受节点被授权参与区块链网络时，验证节点可以继续基于交易记录来更新用户区块链。

[0091] 在704，交易记录可以识别与所接收到的交易记录有关的用户区块链。在一些实施方案中，可以基于提供给验证节点服务器的电子标识符来识别相关用户区块链。一旦识别了适当的用户区块链，验证节点服务器就可以在706将接收到的交易记录附加到所识别的用户区块链上。在一些实施方案中，接收到的交易记录可以在被接收时被附加到用户区块链。在一些实施方案中，附加到用户区块链的交易记录可以不同于验证节点服务器接收到的交易记录，但是可以包括从接收到的交易记录获得的信息。例如，附加到用户区块链的交易记录的格式可以不同于从接受节点接收到的交易记录的格式。在将交易记录附加到所识别的用户记录之后，验证节点服务器可以在708使用与区块链网络相关联的私钥来对交易记录进行签名。上文参考图4更详细地描述了用于生成可以附到交易记录上的签名的示例

过程。

[0092] 在710，一旦所识别的用户区块链已经被更新和签名，就可以将其分布在整个区块链网络中。特别地，可以将更新的用户区块链提供给区块链网络内的每个验证节点以及区块链网络内的至少一些接受节点。例如，可以向代表资源提供商的每个接受节点提供更新的用户区块链，而可以仅向与用户区块链所属的客户端设备相关联的那些接受节点提供更新的用户区块链。

[0093] 图8描绘了根据至少一些实施方案的用于使用在分布式环境内维护的用户区块链来处理交易的示例过程。根据至少一个实施方案，图8的过程800可以至少由图1和图2所描绘的资源提供商计算机104来执行。资源提供商计算机可以是区块链网络的接受节点。代码可以存储在计算机可读存储介质上，例如以包括可由一个或多个处理器执行的多个指令的计算机程序的形式。计算机可读存储介质可以是非瞬态的。

[0094] 过程800可以开始于802，此时，资源提供商计算机(例如，资源提供商操作的服务器)接收到交易请求。在一些实施方案中，可以与电子标识符一起接收交易请求。在一些实施方案中，可以基于与交易请求相关联地提供的用户信息来生成电子标识符(例如，通过组合和散列各种用户数据)。在一些实施方案中，交易请求可以是在资源提供商计算机与特定个人、设备或实体之间发起特定交易/交互的请求。

[0095] 在804，资源提供商计算机可以获得要与交易请求相关联的电子标识符。在一些实施方案中，可以基于由用户提供的用户信息(例如，经由由用户操作的客户端设备)来生成电子标识符。在一些实施方案中，用户可以在交易请求中提供电子标识符。

[0096] 在806，资源提供商计算机可以获得与所识别的用户相关联的电子记录。在一些实施方案中，用户可以与交易请求一起提供用户区块链。在一些实施方案中，资源提供商计算机可以基于电子标识符来查询所存储的用户区块链的存储库(例如，在分布式数据库内)。获得的用户区块链的每个交易记录都可以包括在请求者与另一实体(例如，资源提供商或另一实体)之间发生的交互的指示。交易记录可以包括至少与这种交互和签名有关的许多细节。交易细节可以包括发起实体(即，与其进行交易的资源提供商)的指示。

[0097] 在808，资源提供商计算机可以验证所获得的用户区块链的至少一部分的真实性。在一些实施方案中，资源提供商计算机可以验证用户区块链中的每个交易记录。在一些实施方案中，资源提供商计算机可以仅验证用户区块链内的一部分交易记录(例如，最后的交易记录或交易记录的随机子集)。在一些实施方案中，用户区块链可以由区块链网络的验证节点使用区块链网络的私钥来签名。以这种方式，资源提供商计算机可以使用区块链网络的公钥，并通过独立生成附到交易记录上的签名的一部分，来验证用户区块链中的交易记录。计算实体可以将用户区块链的至少一部分存储在数据库内。例如，资源提供商计算机可以使用接收到的信息来填充数据库条目的多个字段。

[0098] 在810，资源提供商计算机可以基于用户区块链中的交易记录来确定与交易请求中指示的交易相关联的风险级别。例如，资源提供商计算机可以评估与账户相关联的财务能力和/或流动性级别。在一些实施方案中，可以通过将与账户相关联的资产的数量(和/或价值)和与账户相关联的负债进行比较来确定风险级别。在一些实施方案中，一个或多个交易记录可以包括基于由发起资源提供商执行的账户评估来分配给账户的信用分数的指示。应当注意，一旦资源提供商计算机已经接收到用户区块链，本领域技术人员可以通过多种

方式基于该用户区块链内的各种交易记录来确定风险级别。

[0099] 在一些实施方案中，计算实体可以基于发起交易记录的实体来计算与每个识别的交易记录相关联的信任值。信任值可以提供计算实体信任由发起实体提供的信息的程度的定量表示。在一些实施方案中，可以基于发起实体的类型，发起实体的信用等级，发起实体已经存在的时间长度，发起实体提交的总交易记录的数量，或与发起实体相关的任何其他合适的信息，来确定信任值。在一些实施方案中，资源提供商计算机可以过滤或不考虑与未能超过预定信任值阈值的发起实体相关联的交易记录。

[0100] 在一些实施方案中，资源提供商计算机可以基于与同交易记录相关联的发起资源提供商相关联的信任值，将权重分配给特定交易记录内的信息。通过说明性示例，资源提供商计算机可以确定其对银行机构的信任大于对私人老板的信任。在该示例中，它可以将较高的信任值分配给源自于银行机构的用户区块链的交易记录，而将较低的信任值分配给源自于私人老板的用户区块链的交易记录。在该示例中，与根据与私人老板相关联的交易记录所作的信用评估相比，根据与银行机构相关联的交易记录所作的信用评估具有更大的权重。

[0101] 在812，资源提供商计算机可以基于所确定的风险级别来确定是否进行交易请求中指示的交易。例如，计算实体可以确定风险级别是高于还是低于预定风险级别阈值，或者风险级别是否在可接受范围内。在一些实施方案中，一个或多个所识别的交易记录可以包括对风险级别的指示(例如，信用分数)。在这种情况下，资源提供商计算机(假设与交易记录相关联的信任级别高于信任级别阈值)可以接受交易记录中指示的风险级别。在确定应该进行交易之后，在814完成交易。

[0102] 在816处，资源提供商计算机可以生成与交易请求中指示的动作有关的新交易记录，并将该交易记录发送到验证节点以便附加到用户区块链。在一些实施方案中，资源提供商计算机可以在完成所请求的交易时(即，当动作已经被批准时)生成新的交易记录。在一些实施方案中，资源提供商计算机可以生成关于交易被批准还是被拒绝的交易记录，并带有关于交易状态的指示。应当注意，在一些实施方案中，不管是否从与电子记录相关联的账户的用户接收到许可，都可以更新用户区块链。例如，用户区块链可以用作信用报告工具，其中每个交易记录都反映与另一个实体的交互，无论是肯定的还是否定的。在此示例中，资源提供商计算机无需寻求账户持有人的批准即可创建与该账户相关联的新交易记录。根据至少一些实施方案，然后，在接收到所生成的交易记录时，验证节点服务器可以执行上述过程700。

[0103] 本发明的实施方案提供许多技术优点。例如，服务提供商或用户本身可以将特定用户的电子记录提供给资源提供商。但是，即使用户可以访问他或她自己的用户记录，他或她也无法编辑该用户区块链，因为用户区块链随后将无法通过验证。以这种方式，即使资源提供商无法访问传统的信贷机构，甚至是无互联网连接，资源提供商也可以使用用户区块链来执行信用评估或其他类型的评估。用户和资源提供商都可以完全不受限制地访问任何特定的电子记录。因此，本公开提供了一种系统，其中电子记录是完全可访问的，但是仍然是安全的。

[0104] 另外，本公开的系统提供了许多附加优点。例如，该系统可以充当去中心化的信用授权机构，因为服务提供商可以分析电子记录，以便对与特定用户或设备相关的风险级别

做出更准确的确定。在该示例中，服务提供商能够分析在用户和另一实体之间进行的每个交易。服务提供商可以基于其对交易各方的信任级别来确定给予每个交易多少权重。服务提供商不是简单地从征信机构接受信用分数，而是可以访问原始数据，并且可以利用其自己的算法来评估风险。

[0105] 此外，上述数字签名过程对交易的多个数据元素执行多个独立的散列步骤，然后对组合进行散列处理以为交易记录提供安全且不可更改的唯一签名。

[0106] 应当理解，本发明的任何实施方案都可以使用硬件(例如，专用集成电路或现场可编程门阵列)和/或使用计算机软件以控制逻辑的形式实现，其中通用可编程处理器是模块化的或集成的。如本文中所使用，处理器包含单核处理器、在同一集成芯片上的多核处理器，或在单个电路板上或网络化的多个处理单元。基于本公开和本文中所提供的教示，本领域的普通技术人员将知道并且了解使用硬件和硬件与软件的组合来实施本发明的实施方案的其他方式和/或方法。

[0107] 本申请中描述的任何软件组件或功能可被实现为要使用例如Java、C、C++、C#、Objective-C、Swift的任何合适计算机语言或例如Perl或Python的脚本语言，使用例如常规的或面向对象的技术由处理器执行的软件代码。软件代码可作为一系列指令或命令存储在计算机可读介质上以供存储和/或传递，合适的介质包含随机存取存储器(RAM)、只读存储器(ROM)、例如硬盘驱动器或软盘的磁性介质，或例如光盘(CD)或数字通用盘(DVD)的光学介质、闪存存储器等等。计算机可读介质可以是此类存储或传输设备的任何组合。

[0108] 此类程序还可以使用适应于经由包含互联网的符合多种协议的有线、光学和/或无线网络进行传输的载波信号来编码和传输。因此，根据本发明的实施方案的计算机可读介质可以使用以此类程序编码的数据信号来创建。以程序代码编码的计算机可读介质可与兼容设备一起封装或与其他设备分开地提供(例如，经由因特网下载)。任何此类计算机可读介质可以驻留于单个计算机产品(例如，硬盘驱动器、CD或整个计算机系统)上或内，且可存在于系统或网络内的不同计算机产品上或内。计算机系统可以包含用于将本文中所提及的任何结果提供给用户的监视器、打印机或其他合适的显示器。

[0109] 以上描述是说明性的而不是限制性的。在所属领域的技术人员阅读了本公开后，本发明的许多变化将变得显而易见。因此，本发明的范围不应参考以上描述来确定，而是应参考待决的权利要求以及其完整范围或等效物来确定。例如，虽然所描述的实施方案提到了使用电子记录以便评估动作的风险水平，但是电子记录也可以用于访问数据或其他服务。例如，电子记录可用于获得对位置或服务(例如，火车旅行或音乐会)的访问。在该示例中，电子记录可以包括交易记录，该交易记录指示票证已经与账户相关联。

[0110] 在不偏离本发明的范围的情况下，任何实施方案的一个或多个特征可与任何其他实施方案的一个或多个特征组合。

[0111] 除非明确指示有相反的意思，否则“一个/种”或“该/所述”的叙述旨在表示“一个/种或多个/种”。

[0112] 上文所提及的所有专利、专利申请、公开和描述都出于所有目的而以其全文引用的方式并入本文中。不承认它们是现有技术。

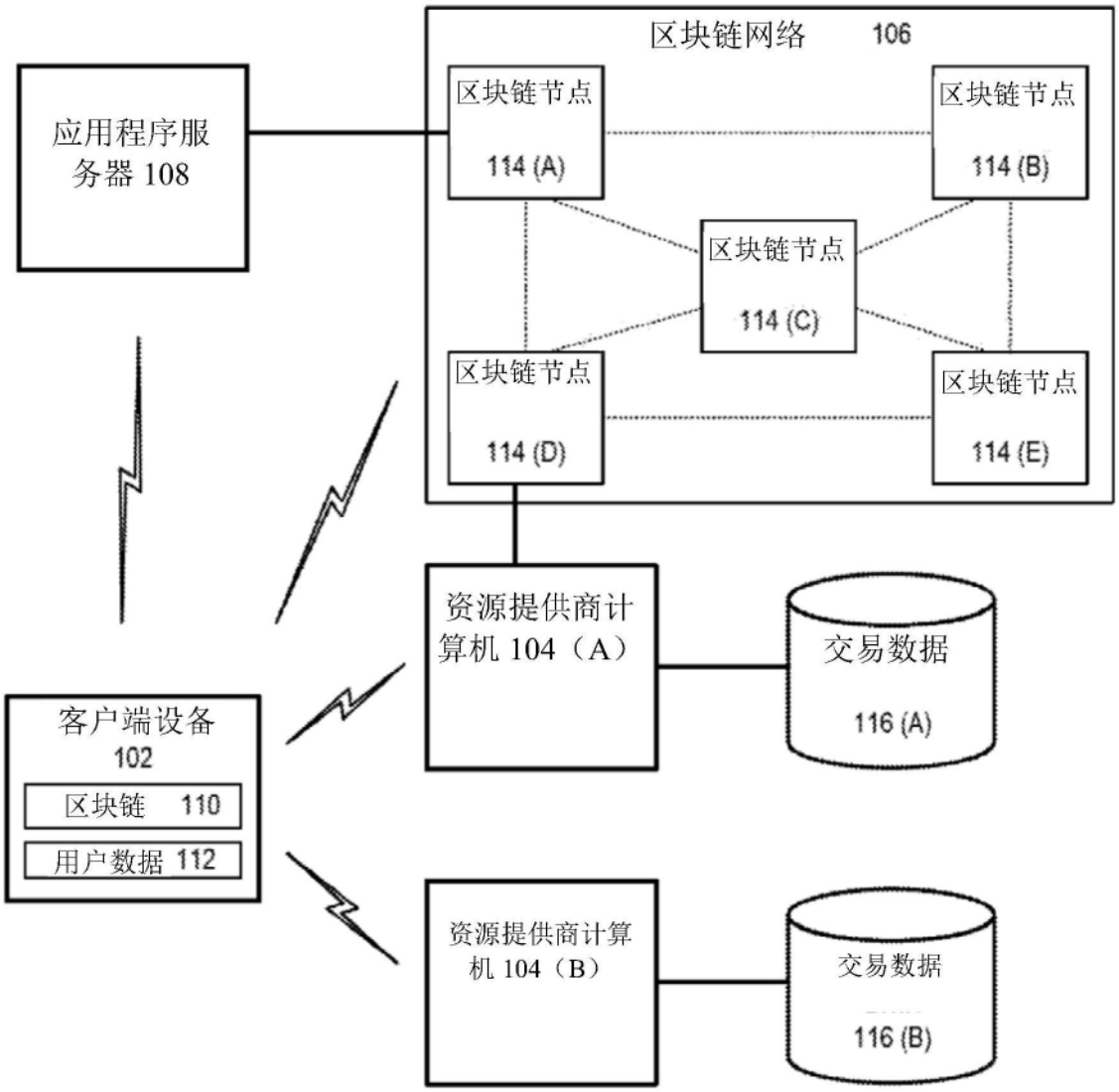

区块链网络 106
应用程序服务器 108
区块链节点 114 (A)
区块链节点 114 (B)
区块链节点 114 (C)
区块链节点 114 (D)
区块链节点 114 (E)
资源提供商计算机 104（A）
交易数据 116 (A)
客户端设备 102
区块链 110
用户数据 112
资源提供商计算机 104（B）
交易数据 116 (B)

图1

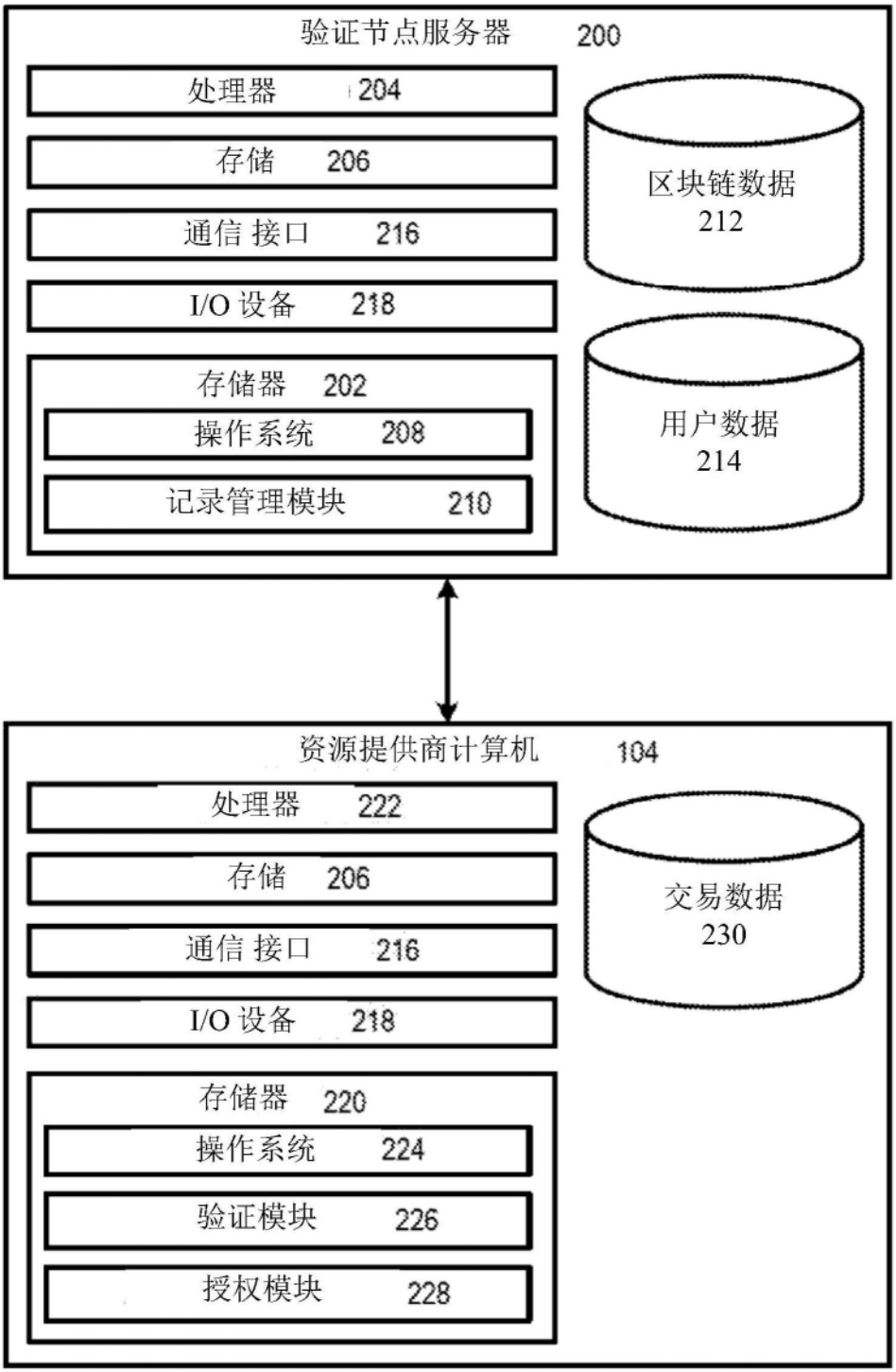

验证节点服务器
200
处理器
204
存储
206
通信 接口
216
I/O 设备
218
存储器
202
操作系统
208
记录管理模块
210
区块链数据
212
用户数据
214
资源提供商计算机
104
处理器
222
存储
206
通信 接口
216
I/O 设备
218
存储器
220
操作系统
224
验证模块
226
授权模块
228
交易数据
230

图2

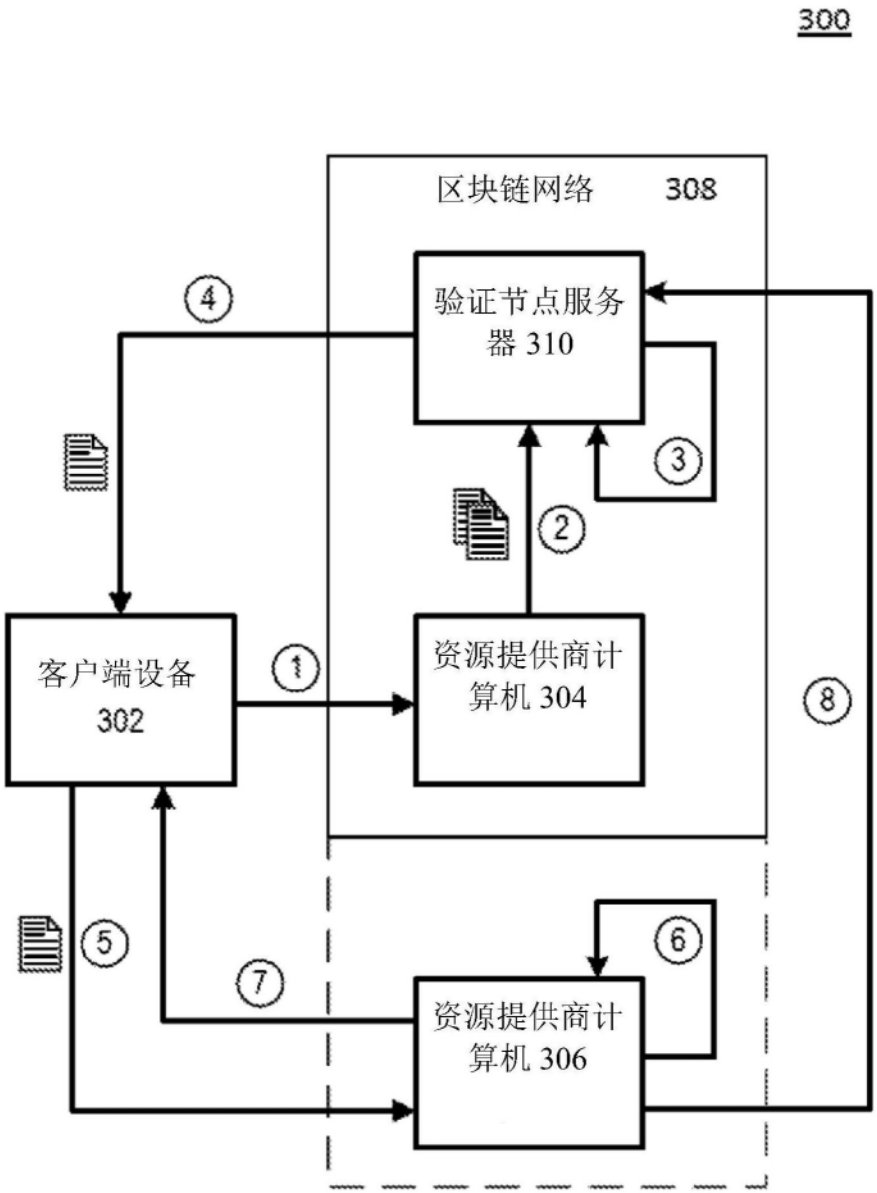

300
区块链网络 308
验证节点服务器 310
客户端设备 302
资源提供商计算机 304
资源提供商计算机 306
1
2
3
4
5
6
7
8

图3

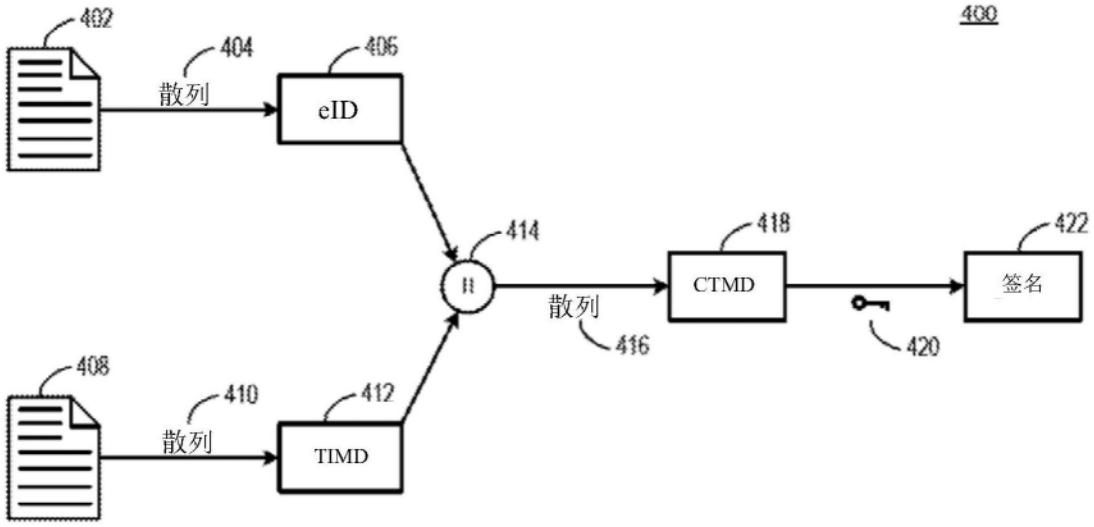

400
402
404
散列
406
eID
414
||
418
CTMD
422
签名
散列
416
420
408
410
散列
412
TIMD

图4

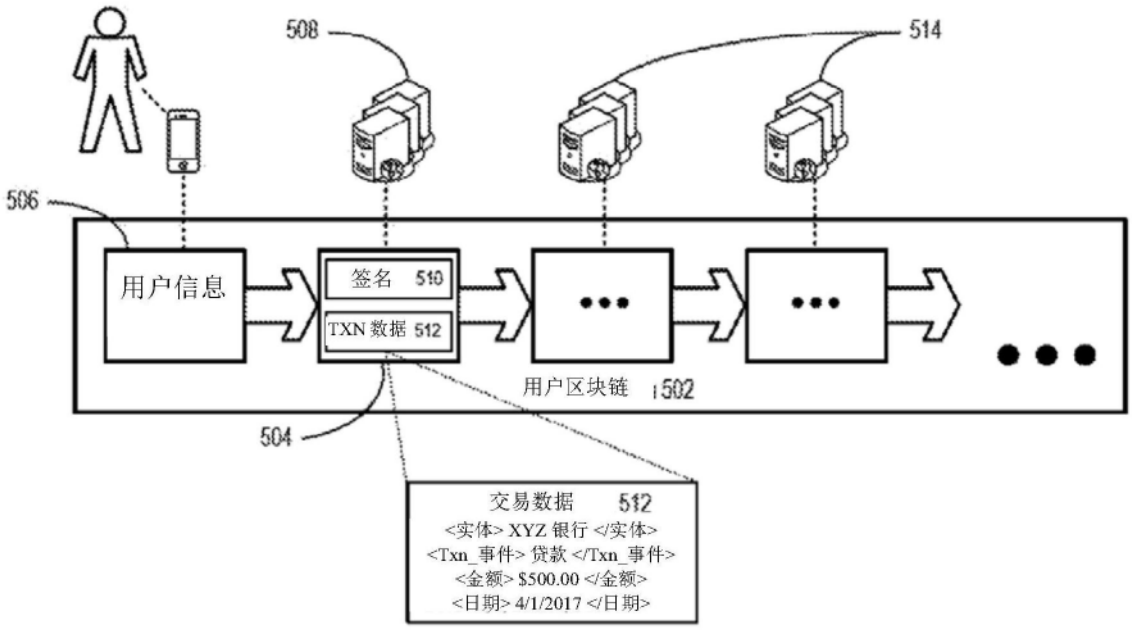

508
514
506
用户信息
签名 510
TXN 数据 512
用户区块链 502
504
交易数据 512
<实体> XYZ 银行 </实体>
<Txn_事件> 贷款 </Txn_事件>
<金额> $500.00 </金额>
<日期> 4/1/2017 </日期>

图5

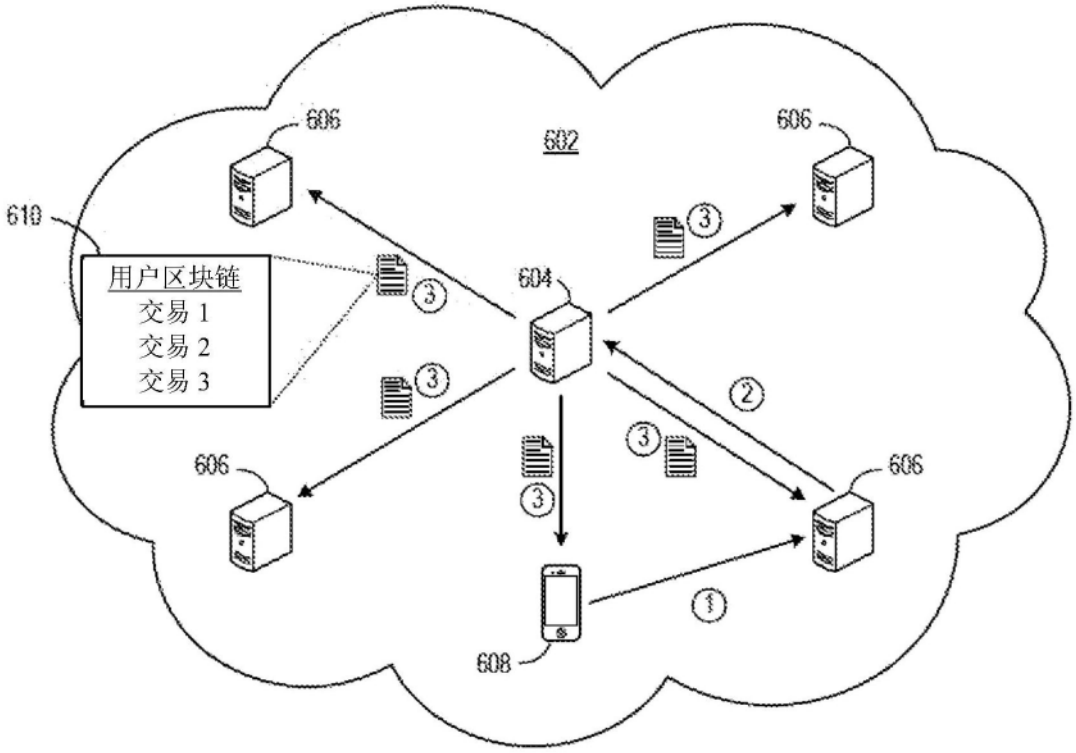


图6

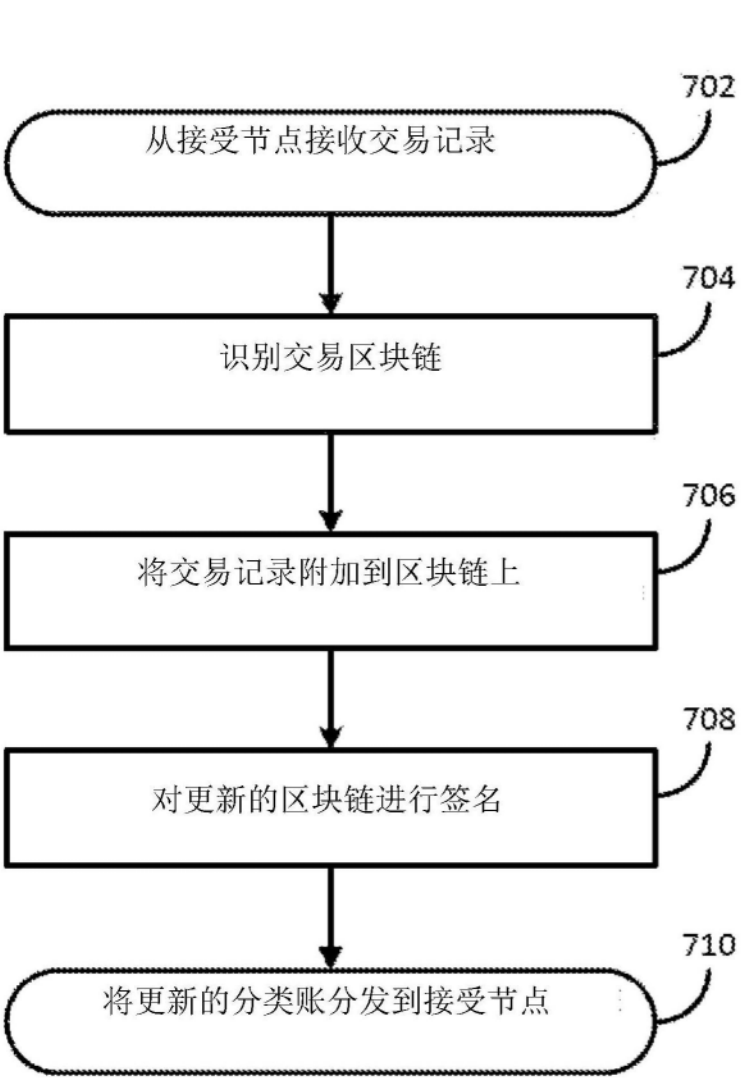

700
702
从接受节点接收交易记录
704
识别交易区块链
706
将交易记录附加到区块链上
708
对更新的区块链进行签名
710
将更新的分类账分发到接受节点

图7

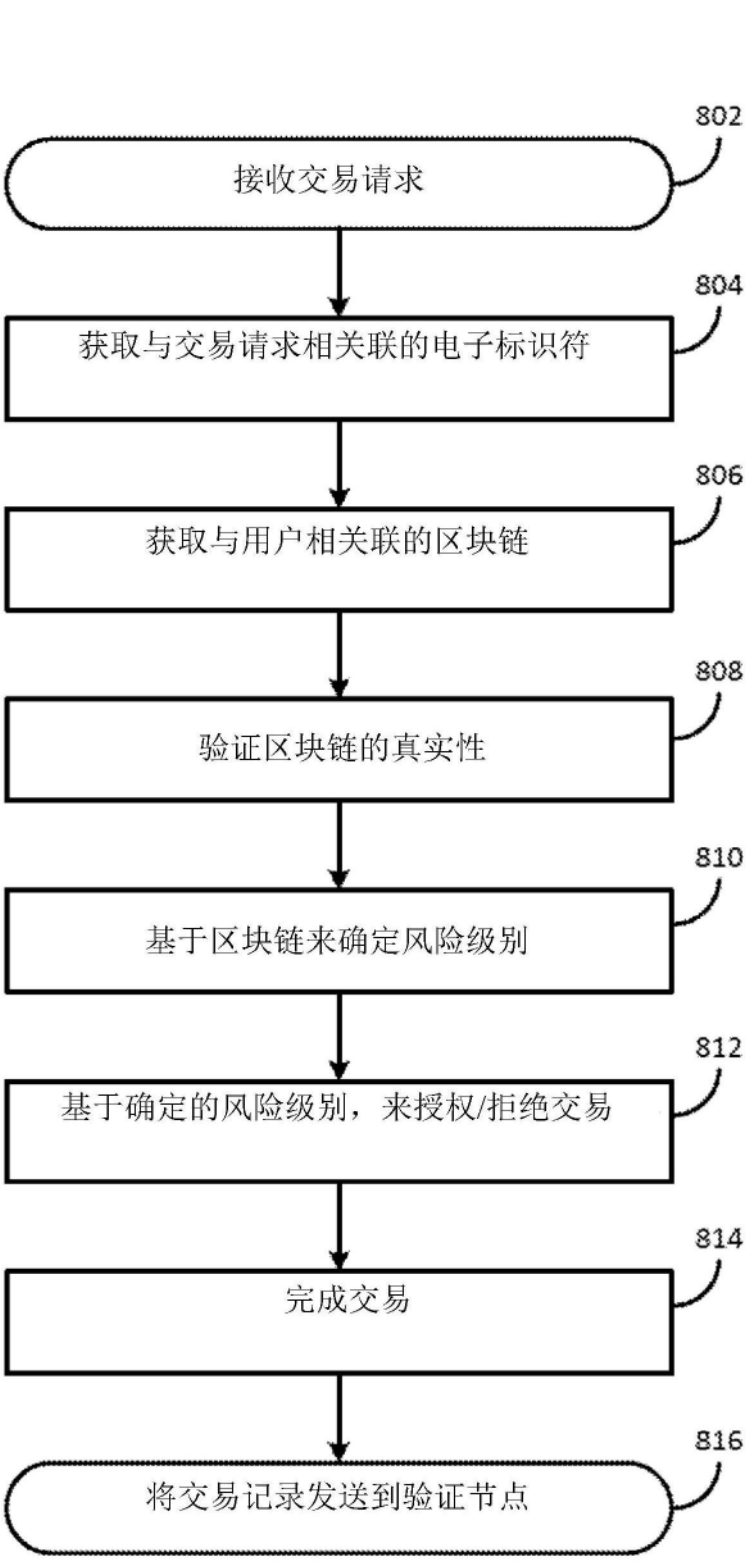

800
802
接收交易请求
804
获取与交易请求相关联的电子标识符
806
获取与用户相关联的区块链
808
验证区块链的真实性
810
基于区块链来确定风险级别
812
基于确定的风险级别，来授权/拒绝交易
814
完成交易
816
将交易记录发送到验证节点

图8