



(12) 发明专利申请

(10) 申请公布号 CN 118172051 A

(43) 申请公布日 2024.06.11

(21) 申请号 202410385127.3

G06Q 50/18 (2012.01)

(22) 申请日 2019.08.12

G06F 21/60 (2013.01)

G06F 21/62 (2013.01)

(62) 分案原申请数据

201980004579.X 2019.08.12

(71) 申请人 创新先进技术有限公司

地址 开曼群岛大开曼岛乔治镇埃尔金大街
190号

(72) 发明人 栗志果

(74) 专利代理机构 北京博思佳知识产权代理有
限公司 11415

专利代理师 李威

(51) Int. Cl.

G06Q 20/10 (2012.01)

G06Q 20/38 (2012.01)

G06Q 40/04 (2012.01)

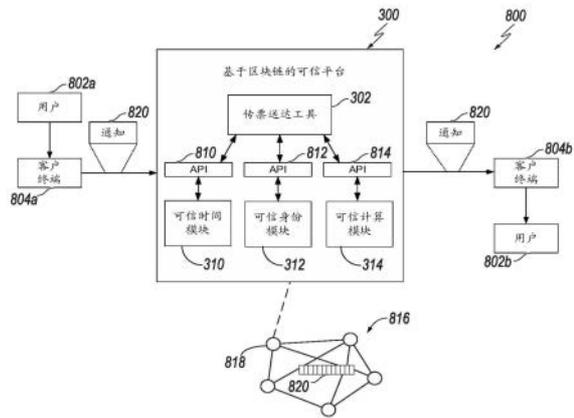
权利要求书4页 说明书53页 附图16页

(54) 发明名称

基于区块链的传票送达

(57) 摘要

本文公开了用于实现基于区块链传票送达的方法、系统和装置,包括编码在计算机存储介质上的计算机程序。所述方法之一包括:接收基于区块链应用生成的请求,该请求用于将与法律诉讼相关的通知从送达方递送到被送达方;基于送达方的身份与送达方的记录在区块链上的注册信息中包含的身份之间的匹配,确定送达方为基于区块链应用的注册用户;将接收到请求的时间记录在区块链上;基于与被送达方相关联的身份,确定被送达方是否为基于区块链应用的注册用户;响应于确定被送达方为注册用户,基于送达方的注册信息和被送达方的注册信息中包含的可用通信方法,识别递送通知的一种或多种方式;及基于一种或多种方式中的至少一种方式向被送达方递送通知。



1. 一种基于区块链的传票送达系统,包括:

基于区块链的传票送达工具,被配置为通过执行多个步骤按照传票送达的法律要求将通知从第一方送达至第二方;以及

可信服务层,包括可信时间模块、可信身份模块和可信计算模块,所述可信服务层用于向所述传票送达工具提供可调用的服务;

其中,所述基于区块链的传票送达工具被配置为,

对于所述多个步骤中的至少一些步骤中的每个步骤,执行以下至少一项:从所述可信时间模块获得经验证时间戳、从所述可信身份模块获得经验证身份、从所述可信身份模块获得计算结果;以及

记录与由所述基于区块链的传票送达工具执行的相应步骤相关联的数据,以及与所述步骤相关联的所述经验证时间戳、所述经验证身份、所述计算结果中的至少一个。

2. 根据权利要求1所述的系统,其中,所述可信计算模块被配置为:

响应于对与向一方送达通知相关联的经验证记录的请求,提供由所述基于区块链的传票送达工具执行的所述多个步骤的经验证记录和与所述多个步骤中的每个步骤相关联的所述经验证时间戳、所述经验证身份、所述计算结果中的至少一个。

3. 根据权利要求1所述的系统,其中,

所述可信计算模块包括具有可信执行环境TEE的一个或多个数据处理器,所述TEE与所述一个或多个数据处理器的操作系统隔离并且被配置为为所述一个或多个数据处理器中执行的代码和加载的数据提供增强的机密性和完整性。

4. 根据权利要求3所述的系统,其中,所述基于区块链的传票送达工具包括:

可信组件,被配置为在所述TEE中执行,并记录由所述基于区块链的传票送达工具执行的所述多个步骤以及与所述多个步骤中的每个步骤相关联的所述经验证时间戳、所述经验证身份、所述计算结果中的至少一个。

5. 根据权利要求4所述的系统,其中,所述可信组件包括:

哈希计算组件,被配置为基于哈希算法生成表示由所述基于区块链的传票送达工具执行的步骤的数据的哈希值。

6. 根据权利要求5所述的系统,其中,所述可信计算模块被配置为:

将所述由所述基于区块链的传票送达工具执行的步骤的数据和所述哈希值添加至存储与所述第一方相关联的经验证记录的区块链。

7. 根据权利要求1所述的系统,其中,所述基于区块链的传票送达工具被配置为:通过与所述可信时间模块、所述可信身份模块或所述可信计算模块相关联的相应的应用编程接口API调用所述可信时间模块、所述可信身份模块或所述可信计算模块的功能。

8. 根据权利要求1所述的系统,其中,所述可信时间模块被配置为:基于(i)国家标准时间信息和/或(ii)从全球定位系统获得的时间信息来生成时间戳。

9. 根据权利要求1所述的系统,其中,所述可信时间模块被配置为:

使用与第一用户相关联的第一法院系统承认的第一标准时间来生成与所述第一用户相关联的时间戳,以及

使用与第二用户相关联的第二法院系统承认的第二标准时间来生成与所述第二用户相关联的时间戳,

所述第一用户和所述第二用户居住在具有不同法院系统的不同区域中。

10. 根据权利要求1所述的系统,其中,所述可信身份模块被配置为基于与用户相关联的一个或多个标识验证所述用户的身份,所述标识包括以下中的至少一个:

- (i) 手机号码、
- (ii) 信用卡号、
- (iii) 与在线支付系统相关联的用户ID、
- (iv) 与在线购物账户相关联的用户ID、
- (v) 与音乐流或下载账户相关联的用户ID、
- (vi) 与电影流或下载账户相关联的用户ID、
- (vii) 与消息传送或聊天账户相关联的用户ID、
- (viii) 与在线银行账户相关联的用户ID、
- (ix) 与约车服务相关联的用户ID、
- (x) 与在线食品订购服务相关联的用户ID、
- (xi) 社会保险号、
- (xii) 驾驶执照号、
- (xiii) 护照号、
- (xiv) 与在线游戏服务相关联的用户ID、
- (xv) 政府实体发布的ID。

11. 根据权利要求1所述的系统,其中,所述可信身份模块被配置为:

使用与第一用户相关联的第一法院系统承认的第一组标识中的至少一个来验证所述第一用户的身份,以及

使用与第二用户相关联的第二法院系统承认的第二组标识中的至少一个来验证所述第二用户的身份,

所述第一用户和所述第二用户居住在具有不同法院系统的不同区域中。

12. 根据权利要求1所述的系统,其中,所述可信计算模块被配置为根据隐私法律记录与用户相关联的信息。

13. 根据权利要求1所述的系统,其中,所述基于区块链的传票送达工具被配置为,在从所述第一方接收到向所述第二方送达通知的请求之后,

调用所述可信身份模块以验证所述第一方的身份和所述第二方的身份,

调用所述可信时间模块以验证用户下订单的时间,以及

调用所述可信计算模块以更新包括表示与传票送达相关联的活动的数据的区块链。

14. 根据权利要求13所述的系统,其中,所述基于区块链的传票送达工具被配置为,在完成将所述通知送达至所述第二方之后,

调用所述可信身份模块以验证所述第二方是实际接收到所述通知的一方,

调用所述可信时间模块以验证所述第二方接收到所述通知的时间,以及

调用所述可信计算模块以更新包括表示与所述传票送达相关联的活动的数据的区块链。

15. 根据权利要求1所述的系统,其中,所述基于区块链的传票送达工具被配置为:

基于与所述系统上注册的所述第二方的一个或多个账户相关联的一种或多种通信方

法,确定用于向所述第二方送达所述通知的方法。

16. 一种基于区块链的传票送达方法,所述方法包括:

接收基于区块链的应用生成的用于将与法律诉讼相关联的通知从送达方递送到被送达方的请求,并将接收到所述请求的时间记录在所述区块链上,所述请求包括与所述送达方相关联的身份和与所述被送达方相关联的身份;

基于与所述送达方相关联的身份确定所述送达方是否为所述基于区块链的应用的注册用户,以及,基于与所述被送达方相关联的身份确定所述被送达方是否为所述基于区块链的应用的注册用户;

响应于确定所述送达方和所述被送达方为注册用户,基于所述送达方的注册信息和所述被送达方的注册信息中包含的可用通信方法对应的至少一种方式,向所述被送达方递送所述通知。

17. 根据权利要求16所述的方法,

所述基于与所述送达方相关联的身份确定所述送达方是否为所述基于区块链的应用的注册用户,包括:在所述送达方的身份匹配于所述送达方的记录在区块链上的注册信息中包含的身份信息的情况下,确定所述送达方为所述基于区块链的应用的注册用户;和/或,

所述基于与所述被送达方相关联的身份确定所述被送达方是否为所述基于区块链的应用的注册用户,包括:在所述被送达方的身份匹配于所述被送达方的记录在区块链上的注册信息中包含的身份信息的情况下,确定所述被送达方为所述基于区块链的应用的注册用户。

18. 根据权利要求17所述的方法,对于所述送达方和所述被送达方中的任一方,所述任一方的记录在区块链上的注册信息中包含的身份信息包括下述至少之一:

与所述任一方相关联的账户的用户ID、与所述任一方相关联的数字密钥、所述任一方的生物特征身份信息。

19. 根据权利要求16所述的方法,还包括:

响应于确定所述被送达方不是所述基于区块链的应用的注册用户,向与所述送达方相关联的账户发送用于指示所述送达方不是注册用户的通知。

20. 根据权利要求16-19中任一项所述的方法,还包括:

在向所述被送达方递送所述通知之后,确定所述被送达方是否已登录在所述基于区块链的应用上注册的账户,以及

响应于确定所述被送达方登录在所述基于区块链的应用上注册的账户,向与所述送达方相关联的账户发送用于指示所述通知已被递送的通知。

21. 根据权利要求20所述的方法,还包括:

响应于确定所述被送达方未登录在所述基于区块链的应用上注册的账户,向与所述送达方相关联的账户发送用于指示所述送达方离线的通知。

22. 根据权利要求16-19中任一项所述的方法,还包括:

在向所述被送达方递送所述通知之前,将所述时间和基于所述时间生成的数字签名添加到所述通知。

23. 根据权利要求22所述的方法,所述数字签名使用与所述送达方相关联的私钥签名

得到。

24. 根据权利要求16-19中任一项所述的方法,所述向所述被送达方递送所述通知,包括:

通过对所述基于区块链的应用所驻留的区块链节点上执行的智能合约进行合约调用来向所述被送达方递送所述通知。

25. 根据权利要求16-19中任一项所述的方法,还包括:

从与所述被送达方相关联的账户接收对接受来自所述送达方的所述通知的确认;

将接收到所述确认的时间记录在所述区块链上;

基于所述送达方的注册信息中包含的所述可用通信方法,向所述送达方递送所述确认。

26. 根据权利要求16-19中任一项所述的方法,其中,所述可用通信方法包括以下中的至少一个:电子邮件、电话呼叫、即时消息传送。

27. 根据权利要求16-19中任一项所述的方法,所述基于区块链的应用由基于区块链的可信平台支持。

28. 一种基于区块链的传票送达装置,所述装置包括用于执行权利要求16-27中任一项所述的方法的多个模块。

基于区块链的传票送达

技术领域

[0001] 本文涉及用于实现传票送达的基于区块链的可信平台。

背景技术

[0002] 分布式账本系统 (DLS), 也可以被称为共识网络和/或区块链网络, 使得参与的实体能够安全地并且不可篡改地存储数据。在不引用任何特定用例的情况下, DLS 通常被称为区块链网络。区块链网络的类型的示例可以包括公有区块链网络、私有区块链网络和联盟区块链网络。联盟区块链网络针对选择的实体组群提供, 该实体组群控制共识处理, 并且联盟区块链网络包括访问控制层。

[0003] 数字网络使世界各地的人们都可以方便有效地找到信息并相互交流。例如, 社交媒体平台使人们可以容易地与朋友和同事共享消息、照片和视频。在线购物网站使消费者可以容易地找到各种产品的信息, 并通过电子方式付款以从世界各地的企业购买产品。新闻网站为用户提供有关世界各地发生的事件的最新信息。媒体平台为用户提供了大量音乐和电影, 以供用户在线下载或流传输。用户可以在线搜索法律服务。约车平台使乘车者能够使用移动电话容易地找到交通工具并移动电话支付交通费用。随着越来越多的人使用互联网并以数字方式进行更多的交易, 欺骗性在线活动的数量和数字交易各方之间的争议也增加了。

[0004] 期望允许用户以方便的方式向法院系统提交与在线数字交易有关的证据。

发明内容

[0005] 本文描述了用于实现可信交易的技术。这些技术通常涉及: 基于区块链的可信平台以多个步骤向用户提供服务; 对于所述多个步骤中的每个步骤, 执行以下至少一项: 从所述可信平台的可信时间模块获得经验证时间戳; 从所述可信平台的可信身份模块获得经验证身份, 或从所述可信平台的可信计算模块获得计算结果; 以及记录与提供给所述用户的所述服务相关联的数据和与所述区块链中的所述步骤相关联的所述经验证时间戳、所述经验证身份或所述计算结果中的至少一项。

[0006] 本文还描述了用于促进传票送达的技术。这些技术通常涉及: 接收基于区块链应用生成的请求, 该请求用于将与法律诉讼相关的通知从送达方递送到被送达方, 其中, 该请求包括与所述送达方相关联的身份和与所述被送达方相关联的身份; 基于所述送达方的身份与所述送达方记录在区块链上的注册信息中包含的身份之间的匹配, 确定所述送达方为所述基于区块链应用的注册用户; 将接收到该请求的时间记录在区块链上; 基于与所述被送达方相关联的身份, 确定所述被送达方是否为所述基于区块链应用的注册用户; 响应于确定所述被送达方为注册用户, 基于所述送达方的注册信息和被送达方的注册信息中包含的可用通信方法, 识别递送所述通知的一种或多种方式; 基于所述一种或多种方式中的至少一种方式, 向被送达方递送该通知。

[0007] 本文还描述了用于法律文档的技术。这些技术通常涉及: 接收从与基于区块链应

用相关联的用户的账户发起的请求,该请求提供服务,其中,该请求包括与该用户相关联的身份;基于所述身份与记录在区块链上的所述基于区块链应用相关联的用户的注册信息中包含的身份之间的匹配,确定所述用户为所述基于区块链应用的注册用户;识别用于提供该服务的多个步骤中要填写并提交的一个或多个电子表格;在所述多个步骤中的每个步骤中:基于执行所述步骤的时间和此时所述电子表格上的数字内容生成唯一标识(ID);将所述唯一ID、所述时间和所述数字内容记录在区块链上;通过更改与所述数字内容相关联的一个或多个属性来表示所述唯一ID,将所述唯一ID嵌入到此时的数字内容中,其中,该嵌入会生成能够基于所述唯一ID从所述区块链检索所述时间和所述数字内容的嵌入信息的数字内容;以及将所述嵌入信息的数字内容记录到区块链。

[0008] 本文还描述了用于争议解决的技术。这些技术通常涉及:在基于区块链应用处,接收用以解决至少第一方和第二方之间的争议的请求,其中,该请求包括与所述第一方关联的第一身份和与所述第二方关联的第二身份;基于所述第一身份与所述第一方的记录在区块链上的注册信息中包含的身份之间的匹配以及所述第二身份与所述第二方的记录在区块链上的注册信息中包含的身份之间的匹配,确定所述第一方和所述第二方是所述基于区块链应用的注册用户;将接收到该请求的时间记录在区块链上;从在所述基于区块链应用中注册的一个或多个争议解决方案提供者接收一个或多个潜在争议解决方案;接收来自所述第一方的第一选择和来自所述第二方的第二选择,其中,所述第一选择包括第一组一个或多个潜在争议解决方案,所述第二选择包括第二组一个或多个潜在争议解决方案;将接收到所述第一选择的时间记录在区块链上和将接收到所述第二选择的时间记录在区块链上;以及确定(i)在所述第一组一个或多个潜在争议解决方案与所述第二组一个或多个潜在争议解决方案之间存在至少一个共同的潜在争议解决方案,和/或(ii)无一潜在争议解决方案是所述第一方和所述第二方均可接受的。

[0009] 本文还描述了用于处理法院判决的技术。这些技术通常涉及:接收与基于区块链应用的账户相关联的请求,所述请求用于收集法院命令中发布的货币裁定(monetary award),其中,所述请求包括与该账户相关联的身份;以及可信身份模块基于与所述命令记录在区块链上的关联哈希值之间的匹配来确定该命令是真实的;可信时间模块将表示接收到所述请求的时间的第一经验证时间戳记录在所述区块链上;调用所述可信计算模块,以基于解析所述命令确定所述货币裁定的债权人、所述货币裁定的债务人和所述货币裁定的金额;基于所述可信身份模块,基于所述身份和记录在所述区块链上的所述账户的注册信息,确定所述账户与所述债权人相关联;调用所述可信计算模块,基于所述注册信息,识别所述债权人的支付账户和所述债务人的一个或多个支付账户,所述债务人的所述一个或多个支付账户的累加余额大于或等于所述货币裁定的金额;调用所述可信计算模块,以将所述货币裁定的金额从所述债务人的所述一个或多个支付账户转账到所述债权人的支付账户;以及所述可信时间模块记录表示所述货币裁定的金额被转账的时间的第二经验证时间戳。

[0010] 本文还提供了用于实现本文提供的方法的系统。所述系统包括一个或多个处理器,以及耦接到所述一个或多个处理器的、其上存储有指令的计算机可读存储介质,当由所述一个或多个处理器执行时,使得所述一个或多个处理器根据本文提供的方法的实施例执行操作。

[0011] 应当理解的是,根据本文的方法可包括本文描述的方面和特征的任何组合。也就是说,根据本文的方法不限于本文具体描述的方面和特征的组合,还包括所提供的方面和特征的任何组合。

[0012] 在附图和以下描述中阐述了本文的一个或多个实施例的细节。根据说明书、附图以及权利要求,本文的其他特征和优点将显现。

附图说明

- [0013] 图1是示出可用于执行本文实施例的环境示例的图。
- [0014] 图2是示出根据本文实施例的架构的示例的图。
- [0015] 图3是示出根据本文实施例的基于区块链的可信平台的示例的图。
- [0016] 图4是示出根据本文实施例的用于收集证据的系统的示例的图。
- [0017] 图5是示出根据本文实施例的用于提供可信时间的系统的示例的图。
- [0018] 图6是示出根据本文实施例的用于提供可信身份的系统的示例的图。
- [0019] 图7是示出根据本文实施例的用于提供传票送达的系统的示例的图。
- [0020] 图8是示出根据本文实施例的用于提供传票送达的系统的另一示例的图。
- [0021] 图9是示出根据本文实施例的处理的示例的流程图。
- [0022] 图10是示出根据本文实施例的用于提供法律文档的系统的示例的图。
- [0023] 图11是示出根据本文实施例的处理的另一示例的流程图。
- [0024] 图12是示出根据本文实施例的用于提供争议解决方案的系统的示例的图。
- [0025] 图13是示出根据本文实施例的处理的又一示例的流程图。
- [0026] 图14是示出根据本文实施例的判决执行的系统的示例的图。
- [0027] 图15是示出根据本文实施例的处理的再一示例的流程图。
- [0028] 图16是示出根据本文实施例的处理的又一示例的流程图。
- [0029] 图17描绘了根据本文实施例的装置的模块的示例。
- [0030] 图18描绘了根据本文实施例的另一装置的模块的示例。
- [0031] 图19描绘了根据本文实施例的又一装置的模块的示例。
- [0032] 图20描绘了根据本文实施例的再一装置的模块的示例。
- [0033] 图21描绘了根据本文实施例的又一装置的模块的示例。
- [0034] 各附图中的相同附图标记和名称表示相同的元件。

具体实施方式

[0035] 本文描述了用于实现可信交易的技术。这些技术通常涉及:基于区块链的可信平台以多个步骤向用户提供服务;对于所述多个步骤中的每个步骤,基于使用可信计算平台的可信计算模块对区块链数据的处理,执行以下至少一项:从所述可信平台的可信时间模块获得经验证时间戳;从所述可信平台的可信身份模块获得经验证身份,或从所述可信平台的可信计算模块获得计算结果;以及记录与提供给所述用户的所述服务相关联的数据和与所述区块链中的所述步骤相关联的所述经验证时间戳、所述经验证身份或所述计算结果中的至少一项。

[0036] 本文还描述了用于促进传票送达的技术。这些技术通常涉及:接收基于区块链应

用生成的请求,该请求用于将与法律诉讼相关的通知从送达方递送到被送达方,其中,该请求包括与所述送达方相关联的身份和与所述被送达方相关联的身份;基于所述送达方的身份与所述送达方的记录在区块链上的注册信息中包含的身份之间的匹配,确定所述送达方为所述基于区块链应用的注册用户;将接收到该请求的时间记录在区块链上;基于与所述被送达方相关联的身份,确定所述被送达方是否为所述基于区块链应用的注册用户;响应于确定所述被送达方为注册用户,基于所述送达方的注册信息和被送达方的注册信息中包含的可用通信方法,识别递送所述通知的一种或多种方式;基于所述一种或多种方式中的至少一种,向被送达方递送该通知。

[0037] 本文还描述了用于法律文档的技术。这些技术通常涉及:接收从与基于区块链应用相关联的用户的账户发起的请求,该请求用于提供服务,其中,该请求包括与该用户相关联的身份;基于所述身份与记录在区块链上的、与所述基于区块链应用相关联的用户的注册信息中包含的身份之间的匹配,确定所述用户为所述基于区块链应用的注册用户;识别用于提供该服务的多个步骤中要填写并提交的一个或多个电子表格;在所述多个步骤中的每个步骤中:基于执行所述步骤的时间和此时所述电子表格上的数字内容生成唯一标识(ID);将所述唯一ID、所述时间和所述数字内容记录在区块链上;通过更改与所述数字内容相关联的一个或多个属性来表示所述唯一ID,将所述唯一ID嵌入到此时的数字内容中,其中,该嵌入会生成能够基于所述唯一ID从所述区块链检索所述时间和所述数字内容的嵌入信息的数字内容;以及将所述嵌入信息的数字内容记录到区块链。

[0038] 本文还描述了用于争议解决的技术。这些技术通常涉及:在基于区块链应用处,接收用以解决至少第一方和第二方之间的争议的请求,其中,该请求包括与所述第一方关联的第一身份和与所述第二方关联的第二身份;基于所述第一身份与所述第一方的记录在区块链上的注册信息中包含的身份之间的匹配,以及所述第二身份与所述第二方的记录在区块链上的注册信息中包含的身份之间的匹配,确定所述第一方和所述第二方是所述基于区块链应用的注册用户;将接收到该请求的时间记录在区块链上;从在所述基于区块链应用中注册的一个或多个争议解决方案提供者接收一个或多个潜在争议解决方案;接收来自所述第一方的第一选择和来自所述第二方的第二选择,其中,所述第一选择包括第一组一个或多个潜在争议解决方案,所述第二选择包括第二组一个或多个潜在争议解决方案;将接收到所述第一选择的时间记录在区块链上以及将接收到所述第二选择的时间记录在区块链上;以及确定(i)在所述第一组一个或多个潜在争议解决方案与所述第二组一个或多个潜在争议解决方案之间存在至少一个共同的潜在争议解决方案,和/或(ii)无一潜在争议解决方案是所述第一方和所述第二方均可接受的。

[0039] 本文还描述了用于处理法院判决的技术。这些技术通常涉及:接收与基于区块链应用的账户相关联的请求,所述请求用于收集法院命令中发布的货币裁定,其中,所述请求包括与该账户相关联的身份;以及可信身份模块基于与记录在区块链上的所述命令相关联的哈希值之间的匹配来确定该命令是真实的;可信时间模块将表示接收到所述请求的时间的第一经验证时间戳记录在所述区块链上;调用所述可信计算模块,以基于解析所述命令确定所述货币裁定的债权人、所述货币裁定的债务人和所述货币裁定的金额;基于所述可信身份模块,基于所述身份和记录在所述区块链上的所述账户的注册信息,确定所述账户与所述债权人相关联;调用所述可信计算模块,基于所述注册信息,识别所述债权人的支付

账户和所述债务人的一个或多个支付账户,所述债务人的所述一个或多个支付账户的累加余额大于或等于所述货币裁定的金额;调用所述可信计算模块,以将所述货币裁定的金额从所述债务人的所述一个或多个支付账户转账到所述债权人的支付账户;以及所述可信时间模块记录表示所述货币裁定的金额被转账的时间的第二经验证时间戳。

[0040] 为本文的实施例提供进一步的背景,如上所述,分布式账本系统(DLS),其也可以称为共识网络(例如,由点对点节点组成)和区块链网络,使参与的实体能够安全地且不可篡改地进行交易和存储数据。尽管术语“区块链”通常与特定网络和/或用例相关联,但是在不参考任何特定用例的情况下,本文使用“区块链”来一般地指代DLS。

[0041] 区块链是以交易不可篡改的方式存储交易的数据结构。因此,区块链上记录的交易是可靠且可信的。区块链包括一个或多个区块。链中的每个区块通过包含在链中紧邻其之前的前一区块的加密哈希值(cryptographic hash)链接到该前一区块。每个区块还包括时间戳、自身的加密哈希值以及一个或多个交易。已经被区块链网络中的节点验证的交易经哈希处理并编入默克尔(Merkle)树中。Merkle树是一种数据结构,在该树的叶节点处的数据经哈希处理,并且在该树的每个分支中的所有哈希值在该分支的根处连接。沿着树持续该处理一直到整个树的根,在整个树的根处存储了代表树中所有数据的哈希值。通过确定哈希值是否与该树的结构一致而可快速验证该哈希值是否为存储在该树中的交易的哈希值。

[0042] 区块链是用于存储交易的去中心化或至少部分去中心化的数据结构,而区块链网络是通过广播、验证和确认交易等来管理、更新和维护一个或多个区块链的计算节点的网络。如上所述,区块链网络可作为公有区块链网络、私有区块链网络或联盟区块链网络被提供。本文参考联盟区块链网络更详细地描述了本文的实施例。然而,可以预期,本文的实施例可以在任何适当类型的区块链网络中实现。

[0043] 通常,联盟区块链网络在参与实体间是私有的。在联盟区块链网络中,共识过程由可被称为共识节点的授权的节点集控制,一个或多个共识节点由相应的实体(例如,金融机构、保险公司)操作。例如,由10个实体(例如,金融机构、保险公司)组成的联盟可以操作联盟区块链网络,每个实体操作联盟区块链网络中的至少一个节点。

[0044] 在一些示例中,在联盟区块链网络内,全局区块链作为跨所有节点复制的区块链被提供。也就是说,所有的共识节点相对于全局区块链处于完全状态共识。为了实现共识(例如,同意将区块添加到区块链),在联盟区块链网络内实现共识协议。例如,联盟区块链网络可以实现实用拜占庭容错(PBFT)共识,下面将进一步详细描述。

[0045] 图1是示出可用于执行本文的实施例的环境100的示例的图。在一些示例中,环境100使能实体能够参与至联盟区块链网络102中。环境100包括计算设备106、108和网络110。在一些示例中,网络110包括局域网(LAN)、广域网(WAN)、互联网或其组合,并且连接网站、用户设备(例如,计算设备)和后端系统。在一些示例中,可以通过有线和/或无线通信链路访问网络110。在一些示例中,网络110使得能够与联盟区块链网络102通信或在联盟区块链网络102内通信。通常,网络110表示一个或多个通信网络。在一些情况下,计算设备106、108可以是云计算设备(未示出)的节点,或者每个计算设备106、108可以是分离的云计算设备,其包括通过网络互连的并且用作分布式处理系统的多个计算机。

[0046] 在所描绘的示例中,计算设备106、108可以各自包括能够作为节点参与至联盟区

区块链网络102中的任何适当的计算设备。计算设备的示例包括但不限于服务器、台式计算机、膝上型计算机、平板计算设备以及智能电话。在一些示例中,计算设备106、108承载一个或多个由计算机实施的服务,用于与联盟区块链网络102进行交互。例如,计算设备106可以承载第一实体(例如,用户A)的计算机实施的、例如交易管理系统的服务,例如第一实体使用该交易管理系统管理其与一个或多个其他实体(例如,其他用户)的交易。计算设备108可以承载第二实体(例如,用户B)的由计算机实施的、例如交易管理系统的服务,例如,第二实体使用该交易管理系统管理其与一个或多个其他实体(例如,其他用户)的交易。在图1的示例中,联盟区块链网络102被表示为节点的点对点网络(Peer-to-Peer network),并且计算设备106、108分别提供参与至联盟区块链网络102中的第一实体和第二实体的节点。

[0047] 图2描绘了根据本文实施例的架构200的示例。示例性概念架构200包括分别对应于参与者A、参与者B和参与者C的参与者系统202、204、206。每个参与者(例如,用户、企业)参与到作为点对点网络提供的区块链网络212中,该点对点网络包括多个节点214,至少一些节点将信息不可篡改地记录在区块链216中。如图中进一步详述,尽管在区块链网络212中示意性地描述了单个区块链216,但是在区块链网络212上提供并维护了区块链216的多个副本。

[0048] 在所描绘的示例中,每个参与者系统202、204、206分别由参与者A、参与者B和参与者C提供或代表参与者A、参与者B和参与者C,并且在区块链网络中作为各自的节点214发挥作用。如这里所使用的,节点通常是指连接到区块链网络212且使相应的参与者能够参与到区块链网络中的个体系统(例如,计算机、服务器)。在图2的示例中,参与者对应于每个节点214。然而,可以预期,一个参与者可以操作区块链网络212内的多个节点214,和/或多个参与者可以共享一个节点214。在一些示例中,参与者系统202、204、206使用协议(例如,超文本传输协议安全(HTTPS))和/或使用远程过程调用(RPC)与区块链网络212通信或通过区块链网络212进行通信。

[0049] 节点214可以在区块链网络212内具有不同的参与程度。例如,一些节点214可以参与共识处理(例如,作为将区块添加到区块链216的矿工节点),而其他节点214不参与此共识处理。作为另一示例,一些节点214存储区块链216的完整的副本,而其他节点214仅存储区块链216的一部分的副本。例如,数据访问特权可以限制相应的参与者在其相应系统内存储的区块链数据。在图2的示例中,参与者系统202、204、206存储区块链216的相应的完整副本216'、216"和216"'。

[0050] 区块链(例如,图2的区块链216)由一系列区块组成,每个区块存储数据。数据的示例包括表示两个或更多参与者之间的交易的交易数据。尽管本文通过非限制性示例使用了“交易”,但是可以预期,任何适当的数据可以存储在区块链中(例如,文档、图像、视频、音频)。交易的示例可以包括但不限于交换有价值的东西(例如,资产、产品、服务、货币)。交易数据不可篡改地存储在区块链中。也就是说,交易数据不能改变。

[0051] 在将交易数据存储于区块中之前,对交易数据进行哈希处理。哈希处理是将交易数据(作为字符串数据提供)转换为固定长度哈希值(也作为字符串数据提供)的处理。不可能对哈希值进行去哈希处理(un-hash)以获取交易数据。哈希处理可确保即使交易数据轻微改变也会导致完全不同的哈希值。此外,如上所述,哈希值具有固定长度。也就是说,无论交易数据的大小如何,哈希值的长度都是固定的。哈希处理包括通过哈希函数处理交易数

据以生成哈希值。哈希函数的示例包括但不限于输出256位哈希值的安全哈希算法(SHA)-256。

[0052] 多个交易的交易数据被哈希处理并存储在区块中。例如,提供两个交易的哈希值,并对它们本身进行哈希处理以提供另一个哈希值。重复此过程,直到针对所有要存储在区块中的交易提供单个哈希值为止。该哈希值被称为Merkle根哈希值,并存储在区块的头中。任何交易中的更改都会导致其哈希值发生变化,并最终导致Merkle根哈希值发生变化。

[0053] 通过共识协议将区块添加到区块链。区块链网络中的多个节点参与共识协议,并执行将区块添加到区块链中的工作。这样的节点被称为共识节点。上文介绍的PBFT用作共识协议的非限制性示例。共识节点执行共识协议以将交易添加到区块链,并更新区块链网络的整体状态。

[0054] 更详细地,共识节点生成区块头,对区块中的所有交易进行哈希处理,并将所得的哈希值成对地组合以生成进一步的哈希值,直到为区块中的所有交易提供单个哈希值(Merkle根哈希值)。将此哈希值添加到区块头中。共识节点还确定区块链中最新的区块(即添加到区块链中的最后一个区块)的哈希值。共识节点还向区块头添加随机数(nonce)值和时间戳。

[0055] 通常,PBFT提供容忍拜占庭错误(例如,故障节点、恶意节点)的实用拜占庭状态机复制。这通过假设错误将在PBFT中发生(例如,假设存在独立的节点失效和/或由共识节点发送的篡改消息)来实现。在PBFT中,在包括主共识节点和备共识节点的序列中提供共识节点。主共识节点被周期性地改变。通过由区块链网络内的所有共识节点对区块链网络的全局状态达成一致,将交易添加到区块链中。在该处理中,消息在共识节点之间传输,并且每个共识节点证明消息是从指定的对等节点接收的,并验证在交易期间消息未篡改。

[0056] 在PBFT中,共识协议是在所有共识节点始于相同的状态的情况下分多个阶段提供的。首先,客户端向主共识节点发送请求以调用服务操作(例如,在区块链网络内执行交易)。响应于接收到该请求,主共识节点将该请求组播到备共识节点。备共识节点执行该请求,并各自向客户端发送回复。客户端等待直到收到阈值数量的回复。在一些示例中,客户端等待接收 $f+1$ 个回复,其中 f 是区块链网络内可以容忍的错误共识节点的最大数量。最终结果是,足够数量的共识节点就将记录添加到区块链的顺序达成一致,该记录被接受或者被拒绝。

[0057] 在一些区块链网络中,用加密处理(cryptography)来维护交易的隐私。例如,如果两个节点想要保持交易隐私,以使得区块链网络中的其他节点不能看出交易的细节,则这两个节点可以对交易数据进行加密处理。加密处理的示例包括(但不限于)对称加密和非对称加密。对称加密是指使用单个密钥既进行加密(从明文生成密文)又进行解密(从密文生成明文)的加密过程。在对称加密中,同一密钥可用于多个节点,因此每个节点都可以对交易数据进行加密/解密。

[0058] 非对称加密使用密钥对,每个密钥对包括私钥和公钥,私钥仅对于相应节点是已知的,而公钥对于区块链网络中的任何或所有其他节点是已知的。节点可以使用另一个节点的公钥来加密数据,并且该加密的数据可以使用其他节点的私钥被解密。例如,再次参考图2,参与者A可以使用参与者B的公钥来加密数据,并将加密数据发送给参与者B。参与者B可以使用其私钥来解密该加密数据(密文)并提取原始数据(明文)。使用节点的公钥加密的

消息只能使用该节点的私钥解密。

[0059] 非对称加密用于提供数字签名,这使得交易中的参与者能够确认交易中的其他参与者以及交易的有效性。例如,节点可以对消息进行数字签名,而另一个节点可以根据参与者A的该数字签名来确认该消息是由该节点发送的。数字签名也可以用于确保消息在传输过程中不被篡改。例如,再次参考图2,参与者A将向参与者B发送消息。参与者A生成该消息的哈希值,然后使用其私钥加密该哈希值以提供为加密哈希值的数字签名。参与者A将该数字签名附加到该消息上,并将该具有数字签名的消息发送给参与者B。参与者B使用参与者A的公钥解密该数字签名,并提取哈希值。参与者B对该消息进行哈希处理并比较哈希值。如果哈希值相同,参与者B可以确认该消息确实来自参与者A,且未被篡改。

[0060] 在一些实施例中,区块链网络中的节点和/或与区块链网络通信的节点可以使用可信执行环境(TEE)来操作。在较高级别,TEE是硬件(一个或多个处理器、内存)内与硬件的操作环境(例如,操作系统(OS)、基本输入/输出系统(BIOS))隔离的可信执行环境。更详细地,TEE是处理器的确保代码执行以及主处理器中加载的数据的私密性和完整性的单独的、安全区域。在处理器内,TEE与OS并行运行。至少部分所谓的可信应用(Trusted Application,TA)在TEE中执行,并且可以访问处理器和存储器。通过TEE,可以保护TA免受主OS中运行的其他应用程序的攻击。此外,TEE在TEE内部将TA相互加密隔离。

[0061] TEE的示例包括美国加利福尼亚州圣塔克拉的英特尔公司提供的软件保护扩展(SGX)。尽管本文通过示例的方式讨论了SGX,但是可以预期,可以使用任何适当的TEE来实现本文的实施例。

[0062] SGX提供了基于硬件的TEE。在SGX中,可信硬件是中央处理器(CPU)的核心,并且物理存储器的一部分被隔离以保护选择的代码和数据。存储器的隔离部分称为飞地(enclave)。更具体地,将飞地作为存储器中的飞地页面高速缓存(enclave page cache, EPC)提供,并映射到应用地址空间。存储器(例如,DRAM)包括用于SGX的保留的随机存储器(PRM)。PRM是BIOS级别最低的连续存储空间,任何软件都无法访问。每个EPC是由OS分配以在PRM中加载应用程序数据和代码的存储集(例如4KB)。EPC元数据(EPCM)是各个EPC的入口地址,并确保每个EPC只能由一个飞地共享。也就是说,单个飞地可以使用多个EPC,而EPC专用于单个飞地。

[0063] 在执行TA期间,处理器在访问存储在飞地中的数据时以所谓的飞地模式运行。飞地模式下的操作会对每次存储器访问执行额外的硬件检查。在SGX中,TA被编译为可信部分和不可信部分。例如,OS、BIOS、特权系统代码、虚拟机管理器(VMM)、系统管理模式(SMM)等无法访问可信部分。在操作中,TA在存储器的PRM中运行并创建飞地。飞地内的可信部分执行的可信函数由不可信部分调用,并且在飞地内执行的代码将数据视为明文数据(未加密),并且拒绝外部访问该数据。可信部分提供对调用的加密响应,并且TA继续执行。

[0064] 可以执行证明处理以验证在提供SGX的TEE中安全地执行了期望的代码(例如TA的可信部分)。通常,证明处理包括从质询者(例如,区块链网络中的另一个节点,区块链网络的密钥管理系统(KMS))接收证明请求的TA。作为响应,TA要求其飞地生成远程证明,也称为举证。生成远程证明包括将本地证明从飞地发送到所谓的举证飞地,该举证飞地对本地证明进行验证,并通过使用非对称证明密钥对本地证明进行签名,从而将本地证明转换为远程证明。远程证明(举证)被提供给质询者(例如,区块链网络的KMS)。

[0065] 质询者使用证明验证服务来验证该远程证明。对于SGX,英特尔提供了英特尔认证服务(IAS),该服务从质询者接收远程证明,并验证该远程证明。更具体地,IAS处理该远程证明,并提供报告(例如,证明验证报告(AVR)),该报告指示是否验证了所述远程证明。如果未验证,则可能指示错误。如果已验证(期望的代码已在TEE中安全执行),则质询者可以开始或继续与TA进行交互。例如,响应于所述验证,KMS(作为质询者)可以将非对称加密密钥(例如,公钥和私钥对)发布给执行TEE的节点(例如,通过诸如椭圆曲线Diffie-Hellman(ECDH)的密钥交换处理),以使节点能够与其他节点和/或客户端安全地通信。在例如2019年4月3日提交的PCT申请PCT/CN2019/081180中描述了TEE技术的额外的细节,其内容通过引用并入。

[0066] 上述区块链和TEE技术可用于生成与在线交易相关的高度可靠的记录。在线交易通常涉及多个步骤。替代生成交易的最终结果的经验证记录(例如生成在交易结束时生成的数据的哈希值),本文中描述的新颖性系统使用在交易的多个步骤中发生的多个事件期间生成的数据以生成可用于验证交易的记录。来源于与交易的多个步骤相关联的事件的数据的经验证记录比仅基于交易的最终结果的经验证记录要可靠得多。在一些实施例中,对于每条需要被验证的数据,不仅每条数据本身被验证,生成每条数据的处理也被验证。生成一条数据的处理可能涉及多个步骤,并且该处理的每个步骤都经过验证。这确保了最终数据是高度可靠的,因为该处理的每个步骤都被欺骗性地修改的概率非常低。在一些实施例中,提供了一种用于以数字数据形式收集证据的工具。对于每条需要被验证的证据,不仅证据本身被验证,收集或生成每条证据的处理也被验证。收集或生成一条证据的处理可能涉及多个步骤,并且该处理的每个步骤都经过验证。这样可以确保在处理结束时收集或生成的证据是高度可靠的,因为有人在该处理的每个步骤中均欺骗性地修改数据的概率非常低。

[0067] 参照图3,本文描述了用于实现基于区块链的可信平台300(可以是可信在线平台)的技术,该可信平台可增强用户之间的信任并提供各种法律服务或处理工具以允许用户以一种有效的方式进行法律诉讼或与法律服务相关的交易。基于区块链的可信平台300提供的法律服务工具包括,例如,基于区块链的传票送达工具302、基于区块链的争议解决工具304、基于区块链的法律文档工具306和基于区块链的判决执行工具308。传票送达工具302允许原告根据传票送达的法律要求数字化地向被告送达通知(例如,送达传票或其他相关文件)。争议解决工具304允许两个或多个争议方以方便的方式从多个争议解决方案提供者(例如,争议调解员)中找到一个或多个潜在(或候选)解决方案。法律文档工具306允许用户根据相关法律要求数字化地填写和提交法律文件。判决执行工具308允许原告根据相关法律要求执行法院判决,例如以数字方式向被告的银行发出银行征款法院命令。工具302、304、306和308被提供在可信平台300的可信应用层322中。可信平台300还包括可信服务层324,该可信服务层324包括:例如可信时间模块310、可信身份模块312和可信计算模块314,以支持可信应用层322中各种法律服务工具的操作。

[0068] 以数字化方式在线进行法律交易的优势在于,交易可以快速、有效地执行,部分原因是无需填写法律文档,也无需通过亲自递送或邮件邮寄的方式递送法律文档。但是,数字数据的短暂性也使得难以以满足法院证据规则的方式认证或验证在线数字化完成的交易。不同于在纸质文档中修改印刷在纸质媒介上的内容通常会留下修改的痕迹,例如纸纤维或

墨水分子的变化,而修改数字文档通常不会留下任何修改痕迹。此外,数字文档可能因硬件错误,例如诸如磁盘驱动器、固态驱动器和/或存储设备之类的存储系统的故障,而被破坏。结果,数字文档的内容、与数字文档相关联的用户的身分以及与数字文档相关联的时间可能是可疑的。

[0069] 存在用于认证在两方之间交换的数字文档的技术,诸如计算数字文档的哈希值以及与两方共享该哈希值。存在用于认证与数字文档相关联的各方的身分的技术,例如使用经验证的数字签名。然而,这种技术在限定情况下可用于验证各个文档的内容和/或与各个文档相关联的各方的身分,但在没有诸如商定的哈希值或经验证的数字签名的情况下,经常会发生法律争议。

[0070] 例如,A方(例如,受版权保护的资料的作者)指控B方(例如,在线出版商)承载的网页包含侵犯A方版权的内容。A方向法院提起诉讼并向法院提交涉嫌包含侵犯版权内容的网页副本。B方否认曾在网页上承载此类侵犯版权的资料,并声称A方修改了用作支持该虚假指控的证据的网页的内容或URL。A方声称,B方在获悉该诉讼后,修改了网站上发布的网页,并删除了该侵犯版权的内容。B方声称,提起诉讼的人不是A方,而是其他没有资格提起诉讼的人。在这种情况下,一方的证据和身分都存在疑问。作为另一示例,C方(例如,卖方)声称D方(例如,买方)在在线跳蚤市场上订购了产品,但从未为该产品付款。C方向法院提起诉讼,并向法院提交了数字订单的副本。D方否认曾经下该订单,并声称该订单是由假装为D方的其他人下的。再例如,E方和F方协商协议,对该协议的早期草案进行了一些修改,并最终签署了该协议的最终版本。整个处理在线完成,无需交换任何纸质文档。后来,E方向法院提起诉讼,声称F方不遵守该协议的某些条款。F方声明其遵守该协议的所有条款,并反驳称E方在对协议进行数字化签名后以欺骗方式修改了该协议。E方和F方产生了最终数字签名协议的两种不同的版本。再举个例子,F方签署了该协议,在将该协议递送到E方正确的电子邮件地址之前,递送到了错误的电子邮件地址直到几天后才发现。然后,E方依赖递送日期来执行该协议而F方则依赖签署协议的日期来执行该协议。当法院收到上述诉讼时,由于难以验证各方提供的证据的真实性,法院可能难以适当地裁定所述争议。

[0071] 在某些示例中,各方可以聘请律师收集证据,并向法院提交宣誓书,以证明证据的真实性。但是,聘请律师并与之协调可能既昂贵又耗时。在某些情况下,争议事件已经发生,相关的数字文档已被更改,甚至律师也难以收集相关证据。

[0072] 基于区块链的可信平台300通过提供一套法律服务应用程序解决了上述问题,该法律服务应用程序利用可信时间模块310、可信身份模块312和可信计算模块314的功能以符合(或比以前的系统更符合)相关证据规则的方式来认证文档和/或用户身份。

[0073] 一些法院系统和政府机构允许公民在线提起法律诉讼。例如,中国杭州的互联网法院受理电子形式的诉讼和备案,并通过直播方式审理案件。不列颠哥伦比亚省民事解决法庭是加拿大的一个在线法庭,可以在线解决某些类型的争议。例如,可信平台300可以与法院系统连接并提供集成的用户界面,从而用户可以以方便的方式向法院系统提起诉讼并提交证据。

[0074] 在一些实施例中,基于区块链的可信平台300的新颖性特征在于:该平台提供可信时间、可信身份和可信计算,以使得提供法律服务的应用程序能够以符合(或比以前的系统更符合)证据规则的方式保存与所述服务在多个步骤中的每个步骤中或关键时间点发生的

事件有关的信息(例如,谁、什么、以及何时)的经验证记录。这些记录可以通过与法律机构、执法机构或争议解决机构相关联的区块链节点的共识,被添加到区块链中。一旦被添加,这些记录就成为不可变的,并且可以被法院或各方作为相应法律服务或程序的证据所信任。

[0075] 例如,有些工具提供了哈希和数字签名功能,以允许用户对数据进行数字签名,以便其他用户可以验证该数据自签名以来没有被更改,并且可以验证对该数据进行签名的用户的身份。然而,仍然存在经数字签名的数据包含错误的可能性,例如,在对数据进行签名之前,该数据已被损坏或篡改而签名者并不知情,或者原始的经数字签名的数据在传输期间被黑客拦截,并被伪造的经数字签名的数据所替代。仅基于经数字签名的数据,可能难以证明或反驳数据的真实性和准确性。因此,可能难以在没有例如来自公证人或有执照的律师的证词的进一步证据的情况下在法律诉讼中使用经数字签名的数据,来证明数据的真实性和准确性。要解决的技术问题是如何提高提供法律服务的在线应用程序所生成的数据的可信度。

[0076] 基于区块链的可信平台300通过捕获提供所述法律服务的过程中的多个步骤中的每个步骤(或几个关键时间点)的快照,增强了通过网络提供法律服务的应用程序产生的数据的可信度,并降低了伪造或篡改的概率,其中,每个快照包括由可信时间模块310和/或可信身份模块312提供的信息,并且使用可信计算模块314将所述快照存储在区块链中,以处理区块链数据。所述快照可以包括例如诸如与在相应步骤中或时间点发生的事件相关联的人、时间和内容的信息。在多个步骤中的每个步骤(或每个时间点)中均进行伪造或篡改的概率比在单个步骤(或时间点)中进行伪造或篡改的概率小得多。可信时间模块310提供可信的或经验证的时间戳,可信身份模块312提供可信的或经验证的身份信息,可信计算模块314确保记录在相关区块链中的数据的可信度。

[0077] 在一些实施例中,模块310、312、314的功能可以由在TEE中执行的一个或多个基于区块链的应用程序或智能合约来调用。TEE由与一个或多个数据处理器的操作系统隔离的一个或多个数据处理器承载,并被配置为一个或多个数据处理器中执行的代码以及加载的数据提供增强的机密性和完整性。在某些示例中,应用程序或智能合约可以通过应用程序接口(API)调用模块的功能。

[0078] 基于区块链的可信平台300产生以下技术效果:基于区块链的可信平台300所支持的法律服务应用程序所提供的与法律服务有关的数据具有较高的可信度(与先前的系统相比)。验证与法律服务有关的各方的身份的数据具有较高的可信度。验证由各方执行的动作的数据具有较高的可信度。验证在提供法律服务期间发生的事件的时间的数据具有较高的可信度。验证在多个步骤中的每个步骤或每个时间点向与法律服务有关的各方显示、提供或由其编辑的文档的数据具有较高的可信度。可以保存提供法律服务期间发生的交易历史的高度可靠的记录,包括对文档的修改历史和来自各方的回应。

[0079] 在一些实施例中,可信服务层324可以包括附加模块,例如可信定位模块,提供指示交易发生在何处的经验证位置。例如,所述可信定位模块可用于证明在特定地理区域发生了侵权行为,并且可以向具有管辖权的法院提起诉讼。例如,可信定位模块可以基于由连接到客户终端404(图4)的经验证GPS接收器提供的数据来生成经验证的位置信息。

[0080] 可信平台300包括附加应用程序,例如,第一应用程序316、第二应用程序318、……、和第N应用程序320,它们利用了可信时间模块310、可信身份模块312和可信计算

模块314的功能。下面描述了第一应用程序316提供可用于在互联网上收集证据的“互联网证据收集网络浏览器”424(图4)的示例。

[0081] 参考图4,在一些实施例中,可以通过诸如互联网的网络400来访问可信平台300。用户402使用客户终端404访问可信平台300,客户终端404可以是例如移动电话、个人计算机或可以连接到网络400的任何计算设备。在一些示例中,可信平台300向尚未在平台300注册的用户提供有限的功能。平台300向已经在平台300注册的用户提供工具302、304、306、308,应用程序316、318、320以及模块310、312、314的更多(例如完整)功能。

[0082] 当在平台300注册时,用户具有用户标识(ID),用于在用户402使用平台300的工具和服务时识别用户402。每个注册用户具有与平台300相关联的账户,并且可以在登录该账户之后访问平台300的功能。在一些示例中,用户可以通过提供诸如用户的电话号码和电子邮件地址之类的个人信息来在平台300注册。在一些示例中,用户可以通过与模块310、312、314可通信地耦接的指纹传感器、麦克风或虹膜扫描仪提供的诸如一个或多个指纹、一个或多个声纹或虹膜信息之类的生物特征信息来在平台300注册。当用户访问可信平台300的功能时,用户可以向可信平台300提供附加信息,并且可信平台300将该附加信息与用户账户相关联。

[0083] 例如,用户402可以提供手机号码,以便用户402可以从移动电话上的可信平台300接收消息。用户402可以提供支付账户信息,以便用户402可以为可信平台300上的服务付费。例如,用户账户可以包括以下一个或多个信息,这些信息可用于验证用户402的身份:(i)手机号码、(ii)信用卡号、(iii)与在线支付系统关联的用户ID、(iv)与在线购物账户关联的用户ID、(v)与音乐流或下载账户相关联的用户ID、(vi)与电影流或下载账户相关联的用户ID、(vii)与消息传送或聊天账户相关联的用户ID、(viii)与在线银行账户相关联的用户ID、(ix)与约车服务相关联的用户ID、(x)与在线食品订购服务相关联的用户ID、(xi)社会保险号、(xii)驾驶执照号、(xiii)护照号、(xiv)与在线游戏服务关联的用户ID、(xv)政府实体发布的ID、(xvi)一个或多个指纹、(xvii)一个或多个声纹、或(xviii)虹膜信息。

[0084] 在图4的示例中,用户402访问互联网证据收集网络浏览器424以搜索和查看互联网400上的网页。网络浏览器的客户端组件(图中未示出)在客户终端404处执行,并提供用于向用户402显示网页并接收用于处理网页的用户指令(例如用于控制网页之间的导航的点击)的用户界面。类似地,在一些实施例中,当用户402访问工具302、304、306或308,或者应用程序318或320时,相应的客户端组件在用户终端404处执行并提供用于与用户402交互的相应的用户界面。

[0085] 例如,用户402使用网络浏览器424来访问发布者的网络服务器408上承载的网页406(包括例如网页406a和406b)。用户402最初可以提供发布者的主页的URL,然后单击网络链接以浏览在网络服务器408上承载的网页。在一些实施例中,当用户402使用互联网证据收集网络浏览器424浏览网页时,网络浏览器424调用可信身份模块312以验证用户402的身份。例如,可信身份模块312可以使用与用户账户相关联的任何数量的信息来验证用户402的身份。例如,可信身份模块312可以使用以下一个或多个信息来验证用户402的身份:(i)手机号码、(ii)信用卡号、(iii)与在线支付系统关联的用户ID、(iv)与在线购物账户关联的用户ID、(v)与音乐流或下载账户相关联的用户ID、(vi)与电影流或下载账户相关联

的用户ID、(vii)与消息传送或聊天账户相关联的用户ID、(viii)与在线银行账户相关联的用户ID、(ix)与约车服务相关联的用户ID、(x)与在线食品订购服务相关联的用户ID、(xi)社会保险号、(xii)驾驶执照号、(xiii)护照号、(xiv)与在线游戏服务关联的用户ID、(xv)政府实体发布的ID、(xvi)一个或多个指纹、(xvii)一个或多个声纹、或(xviii)虹膜信息。

[0086] 例如,每当与用户402使用网络浏览器424有关的预定类型的事件发生时,网络浏览器424就调用可信时间模块310以获得关于该事件何时发生的经验证时间戳。预定类型的事件可以包括,例如,从用户402接收输入、向用户402提供输出以及执行预定类型的动作或计算。从用户402接收输入可以包括,例如,接收网页的URL、从用户402接收点击命令或选择命令、从用户402接收例如复制命令的编辑命令、或者从用户402接收例如保存命令的文件命令。向用户402提供输出可以包括,例如,向用户402显示网页的内容、向用户402播放音频文件或向用户402播放视频文件。

[0087] 因此,每当事件发生时,网络浏览器424就执行用户402请求的动作,还调用可信时间模块310以获得经验证的时间戳,该时间戳指示执行该动作的时间或事件发生的时间,在该事件中,用户402执行预定类型的动作,例如向网络浏览器424提供URL、单击网页406上的网络链接、从网页406复制文本或图像、或从网页406下载内容。网络浏览器424调用可信计算模块314以生成事件的快照,其中,该快照可以采用包含以下记录的格式:用户402的身份、事件的描述(例如对执行的动作的描述)、指示事件何时发生(例如,何时执行该动作)的经验证时间戳以及关于与该动作相关联的网页的信息(例如URL)。可信计算模块314生成所述记录的哈希值,并将包括所述记录和所述哈希值的区块添加到存储与用户402相关联的记录的区块链410。

[0088] 例如,以下事件可以与用户402的浏览活动相关联。

[0089] a. 事件1:用户402将发布者的第一网页406a的URL提供给网络浏览器424。

[0090] b. 事件2:网络浏览器424从网络服务器408检索第一网页406a,并向用户402显示网页406a。

[0091] c. 事件3:用户402单击指向第二网页406b的链接。

[0092] d. 事件4:网络浏览器424从网络服务器408检索第二网页406b,并向用户402显示网页406b。

[0093] e. 事件5:用户402将照片422保存在第二网页406b上并写上注释:“在发布者X的具有URL xxx的网页上找到受版权保护的图片”。

[0094] f. 事件6:用户402退出网络浏览器424。

[0095] 在每个事件发生时,网络浏览器424调用可信时间模块310以获得指示该事件发生时间的经验证时间戳。网络浏览器424调用可信计算模块314以更新区块链410,从而添加具有关于该事件的信息的记录。在该示例中,区块412a存储具有关于事件1的信息的记录,区块412b存储具有关于事件2的信息的记录,区块412c存储具有关于事件3的信息的记录,依此类推。

[0096] 可信平台300与区块链网络416中的节点414之一相关联,其中区块链410是跨区块链网络416复制的。例如,节点414之一可以与维护区块链410的版本的法院计算机服务器418相关联。如果用户402向法院提起诉讼,指控网页406b的发布者侵犯了版权,则法院工作人员可以访问维护在法院计算机服务器418上的区块链410中的记录,以检索上述关于所述

事件1至6的信息。法院工作人员可以确定用户402查看了第二网页406b,并且在第二网页406b上保存了照片422并带有以下注释:“在发布者X的具有URL xxx的网页上找到受版权保护的图片”。因为区块链410中的记录具有较高的可信度,所以法院接受区块链410中的记录所提供的信息作为用户402提交的证据。

[0097] 参考图5,在一些实施方式中,可信时间模块基于由国家标准机构分配的协调世界时(UTC)500或由全球定位系统(GPS)接收器502产生的时间信息来产生经验证的时间戳,其中,全球定位系统(GPS)接收器502从诸如中国维护的北斗导航卫星系统、美国维护的全球定位系统、欧盟维护的伽利略全球导航卫星系统、俄罗斯维护的全球轨道导航卫星系统(GLONASS)和/或日本维护的准天顶卫星系统等定位系统获得时间信息。

[0098] 在一些实施例中,全世界许多国家的用户可以访问可信平台300。不同的国家可能对在法律诉讼中可接受的时间信息具有不同的要求或偏好。例如,北京的法院可以接受从国家时间服务中心提供的UTC时间获得的时间信息,或从北斗导航卫星系统获得的时间信息。纽约的法院可以接受从国家标准技术研究院提供的UTC时间获得的时间信息,或从美国全球定位系统获得的时间信息。可信平台300被配置为确定用户居住地的法律管辖权,并在生成与用户相关联的活动的活动的时间戳时使用对应法院系统可接受的时间基准。在一些示例中,可信平台300允许用户选择要使用哪个时间基准。

[0099] 参考图6,在一些实施例中,可信身份模块312维护包括由注册用户自身提供的关于该注册用户的信息的用户账户数据库600。可信身份模块312还访问其他数据库以验证用户提供的账户信息。例如,可信身份模块312可以访问政府ID数据库602以验证由政府ID的准确性。例如,如果可信身份模块312确定由政府ID与在政府ID数据库602中列出的另一用户的名称或电话号码匹配,则可信身份模块312可以生成指示可能为欺骗性身份的警报消息。在从可信身份模块312接收到警报消息时,工具(例如,302、304、306或308)或应用程序(例如316、318或320)可以向用户请求附加信息,以便验证用户的身份。

[0100] 在一些实施例中,可信平台300可以提供在线银行服务并维护访问在线银行服务的用户的账户的数据库604。可信平台300可以提供在线支付服务,例如支付宝,其允许用户以数字方式支付可信平台300上提供的服务。可信平台300可以维护使用可信平台300上提供的在线支付服务的用户的账户的数据库606。可信平台300可以提供允许用户与家庭成员、亲戚、朋友、同事和/或粉丝联系的社交媒体服务。可信平台300可以维护使用可信平台300上提供的社交媒体服务的用户的账户的数据库608。可信平台300可以提供允许用户与其他人通信的通信服务,例如即时消息传送或聊天服务。可信平台300可以维护使用可信平台300上提供的通信服务的用户的账户的数据库610。可信平台300可以与移动电话公司签订合同,其中,移动电话公司协助验证在注册期间用户提供给可信平台300的移动电话号码和其他账户信息是否与在移动电话公司中注册的相应信息匹配。

[0101] 可信平台300可以提供允许用户在线购买产品的在线购物服务。可信平台300可以维护使用可信平台300上提供的在线购物服务的用户的账户的数据库612。可信平台300可以提供允许用户在线购买产品的在线购物服务。可信平台300可以维护使用可信平台300上提供的在线购物服务的用户账户的数据库612。可信平台300可以提供在线娱乐服务,以允许用户通过下载或流传输音乐或电影来收听音乐或观看电影。可信平台300可以维护使用

可信平台300上提供的在线娱乐服务的用户的账户的数据库614。可信平台300可以维护生物特征数据库616,该数据库存储由用户在注册期间提供的生物特征信息,例如一个或多个指纹、一个或多个声纹或者虹膜信息。

[0102] 在一些实施例中,各种数据库600、602、604、606、608、610、612、614、616可以彼此独立地维护。例如,用户可以修改在线银行账户中的信息,而无需修改在线购物账户中的信息。用户可以在不同的时间段更新不同账户中的信息。同一用户可以针对不同的服务使用不同的用户名或别名。多个用户可以共享同一账户,例如,家庭成员可以共享同一电影流账户。同一用户可以针对一项服务开设多个账户,例如,一个用户可以具有多个移动电话号码、多个电子邮件地址和/或多个消息传送ID。因此,基于单个数据库的信息,可能不足以准确地验证用户的身份。但是,通过组合来自多个数据库的信息,可以更可靠地验证用户的身份。

[0103] 可信平台300的特征在于可信身份模块312尝试使用多个数据库来验证用户的身份,因此增加了由可信身份模块312提供的经验证身份信息的可信度。可信身份模块312可以访问以下中的一个或多个作为验证用户身份的处理的一部分:政府ID数据库602、在线银行账户数据库604、在线支付账户数据库606、社交媒体账户数据库608、移动通信账户数据库610、在线购物账户数据库612、在线娱乐账户数据库614和生物特征数据库616。例如,如果用户在注册期间提供的名称和电子邮件地址与在线银行账户数据库604和/或在线支付账户数据库606中的名称和电子邮件地址不匹配,则可信身份模块312可以生成指示可能为欺骗性身份的警报消息,并且可信平台300可能会向用户请求附加信息,以验证该用户的身份。

[0104] 在一些实施例中,当工具或应用程序调用可信身份模块312以验证用户的身份时,该工具或应用程序将用户的ID和其他信息发送到可信身份模块312,并且可信身份模块312将工具或应用程序提供的用户的ID和其他信息与存储在用户账户数据库600及其他数据库602、604、606、608、610、612、614和616中的用户信息进行比较。如果工具或应用程序提供的用户信息与存储在数据库中的用户信息一致,则可信身份模块312验证了用户的身份。另一方面,如果由工具或应用程序提供的用户信息与存储在一个或多个数据库中的用户信息不一致,则可信身份模块312生成指示该用户的身份不能被验证的警报消息。

[0105] 在一些实施例中,可信身份模块312可以生成信任得分连同经验证身份。例如,如果用户访问可信平台300上的工具或应用程序之一,并且与该用户相关联的账户已经很多年不活跃,则可信身份模块312可以针对该用户的身份生成较低信任得分,因为数据库中的陈旧数据可能并不完全准确。另一方面,如果用户在可信平台300上非常活跃,使用由可信平台300提供的许多服务,并且与该用户相关联的大多数或所有数据库中的账户信息彼此一致,则可信身份模块312可以针对用户的身份生成较高的信任得分,因为大多数或所有数据库中的账户信息始终是欺骗性的概率很小。

[0106] 下面描述使用传票送达工具302来送达通知的示例。参考图7,在一些实施例中,第一用户708(其可以是例如原告或代表原告的律师)使用客户终端710访问可信平台300,客户终端710可以是例如移动电话、个人计算机或可以连接到网络400的任何计算设备。在该示例中,第一用户708先前已经在可信平台300注册。在登录可信平台300之后,第一用户708可以访问传票送达工具302。

[0107] 在一些实施例中,传票送达工具302可以要求用户开设账户并遵循附加的注册处理以提供附加的个人信息,以便验证用户的身份。例如,与传票送达工具302相关联的用户账户可以包括可用于验证用户的身份的以下一个或多个信息:(i) 手机号码、(ii) 信用卡号、(iii) 与在线支付系统关联的用户ID、(iv) 与在线购物账户关联的用户ID、(v) 与音乐流或下载账户相关联的用户ID、(vi) 与电影流或下载账户相关联的用户ID、(vii) 与消息传送或聊天账户相关联的用户ID、(viii) 与在线银行账户相关联的用户ID、(ix) 与约车服务相关联的用户ID、(x) 与在线食品订购服务相关联的用户ID、(xi) 社会保险号、(xii) 驾驶执照号、(xiii) 护照号、(xiv) 与在线游戏服务关联的用户ID、(xv) 政府实体发布的ID、(xvi) 一个或多个指纹、(xvii) 一个或多个声纹、或(xviii) 虹膜信息。

[0108] 假设第一用户708先前已经在传票送达工具302中注册。在登录过程中,传票送达工具302可以调用可信身份模块312以验证第一用户708的身份。在可信身份模块312验证第一用户708的身份之后,传票送达工具302可以向第一用户708授予访问权限。第一用户708可以访问传票送达工具302以将法院发出的文件(例如传票或传讯)送达给另一用户712(第二用户712),该另一用户712可以是例如被告714或该被告的律师。传票送达工具302的客户端组件(图中未示出)可以在客户终端710处执行,并且提供用于与第一用户708交互的用户界面。

[0109] 例如,每当与第一用户708使用传票送达工具302有关的预定类型的事件发生时,传票送达工具302就调用可信时间模块310以获得关于该事件何时发生的经验证时间戳。预定类型的事件可以包括,例如,从第一用户708接收输入、向第一用户708提供输出、向第二用户712发送文档、确认第二用户712对文档的接收以及执行预先指定类型的动作或计算。从第一用户708接收输入可以包括,例如,接收与应当接收通知的所述第二用户712相关联的用户ID或其他个人信息,以及接收来自第一用户708的上传文件(诸如法院发出的传票或传讯)。向第一用户708提供输出可以包括,例如,显示文件已经送达第二用户712的证据,或者显示指示无法联系到第二用户712的消息。

[0110] 如上所述,传票送达工具302可以从可信服务层324调用服务。在一些实施例中,每当事件发生时,例如用户708原告通过传票送达工具302输入身份信息,传票送达工具302就可以调用可信时间模块310以记录指示触发事件发生的时间的经验证时间戳。在一些实施例中,传票送达工具302可以调用可信计算模块314以生成该事件的快照。例如,快照可以包括用户708或712的身份、事件的描述(例如,通过电子邮件发送法律诉讼的通知)、指示触发事件的时间的经验证时间戳、以及补充信息(例如文档格式)等。在一些实施例中,可信计算模块314可以进一步生成与由可信模块310、312、314生成的记录相对应的哈希值。哈希值随后可以被记录到区块链700,使得它们可以被可信平台300的用户用来验证所述记录的真实性。

[0111] 例如,以下事件可以与第一用户708的传票送达活动相关联。

[0112] a. 事件1:第一用户708将第二用户712的用户ID、地址和电话号码提供给传票送达工具302。

[0113] b. 事件2:第一用户708将要送达的文件(例如传票或传讯)上传到传票送达工具302。

[0114] c. 事件3:传票送达工具302确定可用于将文档发送给第二用户712的所有通信方

法。例如,通信方法可以包括将文档发送到第二用户712的一个或多个电子邮件账户、即时消息传送账户或移动电话消息传送账户。

[0115] d. 事件4:传票送达工具302使用传票送达工具302支持的所有可用通信方法将文档发送给第二用户712。

[0116] e. 事件5:传票送达工具302接收到对文档已发送给第二用户712的确认。例如,移动电话消息传送系统可以指示第二用户712在线并且已经接收到文档。

[0117] f. 事件6:可替代地,传票送达工具302可能没有接收到对第二用户712已经接收到文档的任何确认,并且确定第二用户712处于离线状态并且无法联系。

[0118] g. 事件7:传票送达工具302通知第一用户708:文档已经送达第二用户712,或者无法联系到第二用户712。

[0119] 在每个事件发生时,传票送达工具302可以调用可信时间模块310以获得指示该事件发生时间的经验证时间戳。传票送达工具302调用可信计算模块314以更新区块链700,从而添加具有关于该事件的信息的记录。在该示例中,区块702a存储具有关于事件1的信息的记录,区块702b存储具有关于事件2的信息的记录,区块702c存储具有关于事件3的信息的记录,依此类推。在一些实施例中,可以组合多个事件并将其存储在区块链700中的单个区块中。

[0120] 传票送达工具302与区块链网络704中的节点706之一相关联,其中区块链700是跨区块链网络704复制的。例如,节点706之一可以与维护区块链700的版本的法院计算机服务器418相关联。如果用户708通知法院所述传票或传讯已经送达第二用户712,则法院工作人员可以访问维护在法院计算机服务器418上的区块链700中的记录,以检索上述关于所述事件1至7的信息。法院工作人员可以确定第一用户708已将传票或传讯送达第二用户712。因为区块链700中的记录具有较高的可信度,所以法院接受区块链700中的所述记录提供的信息作为第二用户712已被妥善送达通知的证据。

[0121] 传票送达工具302的特征在于可以确定可用于将文档发送给第二用户712的多个通信方法。例如,当用户在可信平台300注册时,可信平台300可以请求用户提供两种或多种联系方式(例如,一个或多个电子邮件地址、一个或多个电话号码(例如,家庭、办公室和移动电话号码)和/或一个或多个消息传送应用的联系信息),以便验证用户的身份。传票送达工具302可以使用第二用户712在注册期间提供给可信平台300的联系方式,以便向第二用户712送达法律通知。另外,当第二用户712使用可信平台300上提供的一个或多个服务时,第二用户712可以不时向那些服务提供更新的联系信息,从而可信平台300可以具有第二用户712的更新的联系信息。

[0122] 在一些实施例中,当传票送达工具302试图向第二用户712递送法律通知时,传票送达工具302可以首先检测第二用户712当前是否已登录可信平台300并使用可信平台300提供的一个或多个服务,以及确定将该法律通知发送给第二用户712的最有效的方法。例如,如果可信平台300检测到第二用户712当前正在使用可信平台300上提供的消息传送服务,则传票送达工具302可以使用该消息传送服务将法院命令文档发送给第二用户712。在一些实施例中,消息传送服务可以具有指示消息已读的内置已读回执功能,并且可以将已读回执发送回传票送达工具302。在一些实施例中,传票送达工具302请求第二用户712手动确认接收并确认身份。第二用户712可以通过提供一个或多个识别信息来确认身份,并且传

票送达工具302调用可信身份模块312以验证第二用户712的身份,从而确保接收法院命令文件的人确实是预期的收件人。传票送达工具302还调用可信时间模块310以生成时间戳,该时间戳指示来自消息传送应用的已读回执的时间或第二用户712确认接收的时间。

[0123] 对于第一用户708来说,使用传票送达工具302是有利的,因为工具302能够使用第一用户708可能不知道的通信方法与第二用户712通信。例如,第一用户708可能仅具有第二用户712的邮寄通讯地址,其中该通讯地址可以是最新的,也可以不是最新的。通过使用传票送达工具302,第一用户708可以使用可信平台300可用的第二用户712的最新联系信息来更有效地向第二用户712送达通知。在一些实施例中,当用户在可信平台300注册时,可信平台300从用户处获得同意可信平台300可以使用用户在注册期间提供的通信方法来送达法律通知的准许。

[0124] 下面描述传票送达工具的另一实施例。图8是示出根据本文的实施例的系统800的示例的图。系统800实现了基于区块链网络的传票送达。一般而言,传票送达是这样的程序:诉讼的一方向另一方(例如被告)、法院或行政机关发出适当的初始法律诉讼通知,以期对该方行使管辖权,从而使该人能够在法院、机关或其他法庭面前对诉讼做出回应。例如,系统800可以被实现为使能从第一方(例如,在客户终端804a上操作的用户802a)向第二方(例如,在客户终端804b上操作的用户802b)递送法律通知(例如,通知820)。

[0125] 作为示例,系统800包括客户终端804a和804b(分别由用户802a和802b使用)、基于区块链的可信平台300和区块链网络816。如图所示,基于区块链的可信平台300包括传票送达工具302,应用编程接口(API)810、812和814,可信时间模块310,可信身份模块312和可信计算模块314。注意,基于区块链的可信平台300被示出为包括传票送达工具302,仅旨在说明。基于区块链的可信平台300可以包括任何合适数量的工具,例如争议解决工具(例如,图3的争议解决工具304)、法律文档工具(例如,法律文档工具306)和判决执行工具(例如,判决执行工具308)等。在一些实施例中,可信平台300与区块链网络816中的节点818之一相关联,其中所述区块链(例如,区块链810)是跨区块链网络816复制的。

[0126] 在一个示例中,用户802a可以使用客户终端804a来向区块链网络816发送网络服务请求(例如,用以向用户802b递送法律通知820的请求)。在区块链网络816中的区块链网络节点818上实现的可信平台300可以处理并满足网络服务请求(例如,经由客户终端804b将通知820递送给用户802b)。

[0127] 客户终端804a和804b可以包括,例如,被编程为执行本文所描述的方法的任何合适的计算机、模块、服务器或计算元件。在一些实施例中,客户终端804a和804b可以包括用于提供客户终端804a和804b的各种功能的网络浏览器或软件应用。

[0128] 可信时间模块310可以被配置为基于国家标准时间信息(例如,格林尼治标准时间(GMT)、UTC)或从全球定位系统获得的时间信息来生成时间戳。

[0129] 在一些实施例中,可信时间模块310可以被配置为使用针对不同区域的法院系统的不同标准时间来生成与不同用户相关联的时间戳。例如,可信时间模块310可以使用与第一用户相关联的第一法院系统承认的第一标准时间来生成与第一用户相关联的时间戳,以及使用与第二用户相关联的第二法院系统承认的第二标准时间来生成与第二用户相关联的时间戳,其中,第一用户和第二用户居住在具有不同法院系统的不同区域中。

[0130] 可信身份模块312可以被配置为基于与用户相关联的一个或多个标识来验证用户

(例如,用户802a和802b)的身份。在一些实施例中,标识可以包括以下中的至少一个:(i) 移动电话号码、(ii) 信用卡号、(iii) 与在线支付系统关联的用户ID、(iv) 与在线购物账户关联的用户ID、(v) 与音乐流或下载账户相关联的用户ID、(vi) 与电影流或下载账户相关联的用户ID、(vii) 与消息传送或聊天账户相关联的用户ID、(viii) 与在线银行账户相关联的用户ID、(ix) 与约车服务相关联的用户ID、(x) 与在线食品订购服务相关联的用户ID、(xi) 社会保险号、(xii) 驾驶执照号、(xiii) 护照号、(xiv) 与在线游戏服务关联的用户ID、(xv) 政府实体发布的ID、(xvi) 一个或多个指纹、(xvii) 一个或多个声纹、或(xviii) 虹膜信息。

[0131] 在一些实施例中,可信身份模块312可以被配置为通过使用不同的标识来验证居住在具有不同法院系统的不同区域中的不同用户。例如,可信身份模块312可以被配置为使用与第一用户相关联的第一法院系统承认的第一组标识中的至少一个来验证第一用户的身份,以及使用与第二用户相关联的第二法院系统承认的第二组标识中的至少一个来验证第二用户的身份,其中,第一用户和第二用户居住在具有不同法院系统的不同区域中。

[0132] 在一些实施例中,可信计算模块314可以包括具有TEE的一个或多个数据处理器,该TEE与一个或多个数据操作系统的操作系统隔离并且被配置为为一个或多个数据处理器中执行的代码和加载的数据提供增强的机密性和完整性。

[0133] 在一些实施例中,可信计算模块314可以被配置为根据隐私法律记录与用户相关联的信息。例如,可信计算模块314可以生成所述记录的哈希值,并将包括所述记录和所述哈希值的区块添加到存储与用户802a相关联的记录的区块链820。

[0134] 在一些实施例中,可信计算模块314可以被配置为响应于对与将所述通知送达至待送达方相关的经验证记录请求,提供由传票送达工具302执行的步骤/操作的经验证记录。可信计算模块314还可以提供与由传票送达工具302执行的步骤/操作中的每个步骤/操作相关联的经验证时间戳、经验证身份和/或计算结果。

[0135] 在一些实施例中,传票送达工具302可以允许送达方(例如,诸如用户802a的原告)根据传票送达的法律要求向要被数字化地送达的一方(例如,诸如用户802b的被告)送达通知(例如,送达传票或其他相关文档诸如通知820)。在一些实施例中,传票送达工具302可以获得并记录由传票送达工具302执行的针对传票送达的多个步骤中的每个步骤的经验证时间戳、经验证身份和/或计算结果。传票送达工具302可以从可信时间模块310获得经验证时间戳,从可信身份模块312获得经验证身份,以及从可信计算模块314获得计算结果。

[0136] 在一些实施例中,传票送达工具302可以包括被配置为在可信执行环境中执行并记录由传票送达工具302执行的步骤、以及记录与所述步骤的每个步骤相关联的经验证时间戳、经验证身份和/或计算结果的可信组件(未示出)。在一些实施例中,可信组件可以包括被配置为基于哈希算法生成表示由传票送达工具执行的步骤的数据的哈希值的哈希计算组件。

[0137] 在一些实施例中,传票送达工具302可以被配置为通过与可信时间模块310、可信身份模块312或可信计算模块314相关联的相应的应用编程接口(API)(例如,API 810、812和814)调用可信时间模块310、可信身份模块312或可信计算模块314的功能。在一些实施例中,API 810、812和814可以包括任何合适的API,诸如表征状态转移(Representational State Transfer, REST)网络API(或RESTful API)或基于简单对象访问协议(SOAP)的网络API等。

[0138] 在一些实施例中,传票送达工具302可以在接收到用于从第一方(例如用户802a)向第二方(例如,用户802b)送达通知的请求之后,调用可信身份模块312以验证第一方的身份和第二季的身份。传票送达工具302可以进一步调用可信时间模块310以验证用户下订单的时间,并且调用可信计算模块314以更新包括表示与传票送达相关联的活动的数据的区块链820。

[0139] 在一些实施例中,传票送达工具302可以被配置为调用可信身份模块312,以在完成向第二季送达通知之后验证第二季是实际上接收到该通知的一方。传票送达工具302可以进一步被配置为调用可信时间模块310以验证第二季接收到该通知的时间,并且调用可信计算模块314以更新包括表示与传票送达相关联的活动的数据的区块链820。

[0140] 在一些实施例中,传票送达工具302可以被配置为基于与系统上注册的第二方的一个或多个账户相关联的一种或多种通信方法,确定用于向第二季送达通知的方法,诸如通过使用第二季的一个或多个电子邮件地址、一个或多个电话号码或者一个或多个消息传送应用的用户标识。

[0141] 在图8的示例中,在一些实施例中,用户802a可以登录可信平台300,并且可信平台300可以提供可用服务的菜单,或者示出具有表示可用工具和应用程序的图标的桌面。用户802a可以使用菜单或图标选择其中一个服务,例如传票送达,在其上执行传票送达工具302。用户802a可以使用传票送达工具302来送达。可信平台300可以与区块链816相关联,传票送达工具302可调用可信计算模块314来处理区块链数据并在区块链816中记录相关数据。传票送达工具302可用于递送除法院命令通知以外的文件。

[0142] 图9是示出根据本文实施例的处理900的示例的流程图。为方便起见,处理900将被描述为由位于一个或多个位置并根据本文被适当地编程的一个或多个计算机的系统执行。例如,诸如图8的系统800的、被适当地编程的分布式系统可以执行处理900。

[0143] 在步骤902,在基于区块链应用处接收用于将与法律诉讼相关联的通知(例如,通知820)从送达方(例如,用户802a)递送到被送达方(例如,用户802b)的请求。在一些实施例中,基于区块链应用由基于区块链的平台支持。例如,基于区块链应用可以是传票送达工具302,并且基于区块链的平台可以是基于区块链的可信平台300。在一些实施例中,用户802a通过选择用于递送法律通知的基于区块链应用的功能来生成请求。在一些实施例中,该请求可以包括与送达方相关联的身份以及与被送达方相关联的身份。该请求还可以包括被送达方的联系信息。

[0144] 在步骤904,确定送达方是否是基于区块链应用或基于区块链的平台的注册用户。在一些实施例中,基于区块链应用可以调用可信身份模块(例如,可信身份模块312)以验证送达方的身份,从而确定送达方是否是基于区块链应用或基于区块链的平台的注册用户。在一些实施例中,该确定可以基于将送达方的身份与送达方的记录在区块链(例如,区块链810)上的注册信息中包括的身份进行匹配。在一些实施例中,用户(例如,用户802a和802b)的记录在区块链上的注册信息可以包括用户的身份信息。身份信息可以包括与用户相关联的账户的用户ID、生物特征身份信息(例如,指纹、面部数据、视网膜图案)以及与用户相关联的数字密钥等。

[0145] 在一些实施例中,注册信息可以包括与用户相关联的可用通信方法。可用通信方法可以包括以下至少一种:电子邮件、电话呼叫或即时消息传送。例如,用户802a的注册信

息可以包括与用户802a相关联的电子邮件地址,与用户802a相关联的电话号码和/或与用户802a相关联的即时消息传送账户。在一些实施例中,可以在注册期间为用户验证注册信息中的身份信息和可用通信方法,以确定他们是真实的。

[0146] 在一些实施例中,基于区块链应用可以调用可信计算模块(例如,可信计算模块314)以更新包括表示与处理900相关联的事件或活动的数据的区块链。例如,基于区块链应用可以调用可信计算模块以将步骤904中的确定的一个或多个计算结果的数据记录在区块链中。

[0147] 如果确定送达方不是基于区块链应用的注册用户,则处理900进行到步骤906,其中向送达方发送通知以指示该送达方不是基于区块链应用的注册用户。如果确定送达方是基于区块链应用的注册用户,则处理900进行到步骤908。

[0148] 在步骤908,在区块链上记录接收到该请求的时间。在一些实施例中,基于区块链应用可以调用可信时间模块(例如,可信时间模块310)以生成与该请求相关联的时间戳。在一些实施例中,可信时间模块310可以使用与送达方相关联的法院系统承认的标准时间(例如,UTC)来生成与来自送达方(例如,用户802a)的请求相关联的时间戳。在一些实施例中,可信时间模块310可以基于从全球定位系统获得的时间信息来生成时间戳。

[0149] 在一些实施例中,时间和基于时间生成的数字签名可以被添加到通知中。在一些实施例中,数字签名可以包括使用与送达方相关联的私钥签名的时间。

[0150] 在步骤910,确定被送达方是否是基于区块链应用的注册用户。在一些实施例中,基于区块链应用可以调用可信身份模块(例如,可信身份模块312)以验证被送达方的身份,从而确定被送达方是否是基于区块链应用的注册用户。在一些实施例中,该确定可以基于将被送达方的身份与被送达方的记录在区块链(例如,区块链810)上的注册信息中包括的身份进行匹配。如果确定被送达方不是基于区块链应用的注册用户,则处理900进行到步骤912,其中向送达方发送通知以指示该被送达方不是基于区块链应用的注册用户。如果确定被送达方是基于区块链应用的注册用户,则处理900进行到步骤914。

[0151] 在914,如果确定被送达方是基于区块链应用的注册用户,则识别出一种或多种递送通知的方式。在一些实施例中,该识别可以基于被送达方的注册信息中包含的一种或多种可用通信方法。例如,基于区块链应用可以确定被送达方的可用通信方法包括电子邮件、电话呼叫和/或即时消息传送,并识别与被送达方相关联的电子邮件地址、电话号码和即时消息传送账户。

[0152] 在916,在向被送达方递送通知之后,确定被送达方是否登录在基于区块链应用中注册的账户。如果确定被送达方未登陆到该账户,则处理900进行到步骤918,其中向送达方发送通知以通知:该被送达方离线。在一些实施例中,可以将通知发送到与送达方相关联的账户,以通知:被送达方离线。在一些实施例中,如果确定被送达方未登陆到该账户,则基于区块链应用可以尝试在其他时间向该被送达方递送通知。如果确定被送达方登陆到该账户,则处理900进行到步骤920。

[0153] 在步骤920,向被送达方递送该通知。在一些实施例中,如果被送达方使用具有内置通信方法的服务登陆基于区块链应用的账户或基于区块链的平台,则该应用使用内置的通信方法尝试向被送达方递送该通知。例如,在918如果应用确定被送达方已登录平台提供的即时消息传送账户,则该应用可以将通知递送到被送达方的即时消息传送账户。在一些

实施例中,可以基于在步骤914确定的一种或多种递送通知的方式中的至少一种方式,向被送达方递送该通知。在一些实施例中,可以使用在步骤914所识别的通信方法同时或并行地向被送达方递送通知。例如,可以通过将通知同时发送到被送达方的电子邮件地址、呼叫被送达方的电话号码以及向被送达方的即时消息传送账户发送即时消息来向被送达方递送通知。

[0154] 在一些实施例中,可以通过对基于区块链应用所驻留的区块链节点(例如,区块链节点818)上执行的智能合约(未示出)进行合约调用来向被送达方递送该通知。智能合约可以包括定义函数或操作来检索、生成、存储、或以其他方式操纵或管理区块链数据。在一些实施例中,当满足一些预定执行条件时,智能合约可以自动执行。例如,当在步骤914中识别出一种或多种递送通知的方式时,智能合约可以使用可用通信方法自执行并向被送达方递送通知。

[0155] 在步骤922,从被送达方接收对接受该通知的确认。例如,如果将该通知递送到被送达方的即时消息传送账户,则当被送达方阅读包含该通知的消息时,即时消息传送程序可以生成已读回执。在一些实施例中,通知请求被送达方通过例如单击消息中指示接收到通知的按钮或发送确认接收的回复消息来手动确认接收。

[0156] 在步骤924,在从被送达方接收到对接受该通知的确认之后,向送达方发送通知以通知:通知已被递送。在一些实施例中,可以将该通知发送到与送达方相关联的账户,以通知:已递送该通知。在一些实施例中,可以基于送达方的注册信息中包含的可用通信方法向送达方递送该确认。

[0157] 在一些实施例中,确认被接收的时间可以被记录在区块链上。例如,基于区块链应用可以调用可信时间模块310以验证接收到确认的时间,并在验证的基础上记录确认被接收的时间。

[0158] 在一些实施例中,基于区块链应用可以调用可信身份模块312以验证被送达方是实际接收到该通知的一方。例如,基于区块链应用可以验证确认中包括的身份信息或数字签名,以确定是否从被送达方接收到该确认。

[0159] 在一些实施例中,基于区块链应用可以调用可信计算模块以更新包括表示与处理900相关联的数据的区块链。例如,基于区块链应用可以调用可信计算模块314以将步骤902-924中的任一步骤的计算结果的数据记录在区块链中。

[0160] 下面描述一个示例,其中用户使用法律文档工具306填写电子表格。在此示例中,填写电子表格的每个步骤都记录到了区块链中,并且是可验证的。在每个步骤中都会生成唯一的ID,并将其嵌入电子表格的数字内容中。唯一的ID可用于检索每个步骤的记录。

[0161] 法律文档工具的实施例使用户和服务提供者能够完成电子表格,例如,作为向用户提供服务的处理的一部分所需的法律文档。传统技术的问题之一在于电子表格的数字内容容易被篡改。在填写数字表格时,也难以验证身份和时间。因此,一些法律文档要求用户和/或服务提供者填写一个或多个纸质表格,这通常需要用户和/或服务提供者相见并一起完成表格。线下完成纸质表格使得服务效率低下,并且难以保存纸质表格。

[0162] 本文中描述的技术产生若干技术效果。在一些实施例中,系统记录用于填写服务的电子表格的每个步骤,例如用户在每个步骤填写的电子表格、在每个步骤的时间以及电子表格在每个步骤上的数字内容。该记录能够验证填写电子表格的每个步骤,从而防止用

户篡改电子表格的内容、伪造电子表格或在填写电子表格时提供欺骗性信息。可以增强服务所需的电子表格的数据完整性和安全性。随着数据的完整性和安全性增强,电子表格可以代替使用以前的技术完成服务所需要的纸质表格。

[0163] 在一些实施例中,在每个步骤都会生成唯一的ID,并将其嵌入电子表格的数字内容中。可以从电子表格中提取唯一ID,以在每个步骤从区块链检索电子表格的时间和数字内容。因此,可以查询并验证电子表格在每个步骤的状态。进一步增强了电子表格的真实性。

[0164] 图10是示出根据本文实施例的用于提供法律文档的系统1000的示例的图。系统1000实现了基于区块链网络的法律文档处理。通常,法律文档处理是用户和/或服务提供者填写与服务提供者提供的服务相对应的一种或多种电子形式的法律文档的程序。

[0165] 作为示例,系统1000包括客户终端1004a和1004b(分别由用户1002和服务提供者1004使用)、基于区块链的可信平台300和区块链网络1016。如图所示,基于区块链的可信平台300包括法律文档工具306,API 810、812和814,可信时间模块310、可信身份模块312和可信计算模块314。注意,基于区块链的可信平台300被示出为包含了法律文档工具306,仅旨在说明。基于区块链的可信平台300可以包括任何合适数量的工具,例如传票送达工具(例如图3的传票送达工具302)、争议解决工具(例如,图3的争议解决工具302)和判决执行工具(例如,判决执行工具308)等。在一些实施例中,可信平台300与区块链网络1016中的节点1014之一相关联,其中区块链(例如区块链1010)是跨区块链网络1016复制的。

[0166] 在一个示例中,用户1002可以使用客户终端1004a来向区块链网络1016发送服务请求(例如,用以为服务填写法律文档的请求)。在区块链网络1016中的区块链网络节点1014上实现的可信平台300可以处理并满足服务请求(例如,为服务填写法律文档的请求)。

[0167] 在一些实施例中,法律文档工具306可以被配置为采用SM2算法,该SM2算法是基于椭圆曲线的公钥加密算法,以对数据通信进行加密并验证身份。在一些实施例中,可以为法律文档工具306记录的内容指定访问级别。某些记录的内容只能由具有指定访问级别的人员访问。

[0168] 客户终端1004a和1004b可以包括,例如,执行本文所描述的方法的任何合适的计算机、模块、服务器或计算元件。在一些实施例中,客户终端1004a和1004b可以包括用于提供客户终端1004a和1004b的各种功能的网络浏览器和软件应用。

[0169] 可信时间模块310可以被配置为从诸如国家时间服务中心(NTSC)、UTC、GPST、GLONASS时间(GLONASS)、伽利略系统时间(GST)或北斗时间(BDT)的时间源获得时间。在一些实施例中,区块链网络可以从单个源获得时间,使得区块链网络中的所有区块链节点可以被同步为同一时间。

[0170] 在一些实施例中,可信时间模块可以被配置为基于(i)国家标准时间信息和/或(ii)从全球定位系统获得的时间信息来生成时间戳。

[0171] 在一些实施例中,可信时间模块310可以被配置为使用针对不同区域的法院系统的不同标准时间来生成与不同用户相关联的时间戳。例如,可信时间模块310可以使用与第一用户相关联的第一法院系统承认的第一标准时间来生成与第一用户相关联的时间戳,以及使用与第二用户相关联的第二法院系统承认的第二标准时间来生成与第二用户相关联的时间戳,其中,第一用户和第二用户居住在具有不同法院系统的不同区域中。

[0172] 可信身份模块312可以被配置为基于与用户或服务提供者相关联的一个或多个标识来验证用户(例如用户1002)的身份或服务提供者(例如,服务提供者1004)的身份。在一些实施例中,标识可以包括以下中的至少一个:(i) 手机号码、(ii) 信用卡号、(iii) 与在线支付系统关联的用户ID、(iv) 与在线购物账户关联的用户ID、(v) 与音乐流或下载账户相关联的用户ID、(vi) 与电影流或下载账户相关联的用户ID、(vii) 与消息传送或聊天账户相关联的用户ID、(viii) 与在线银行账户相关联的用户ID、(ix) 与约车服务相关联的用户ID、(x) 与在线食品订购服务相关联的用户ID、(xi) 社会保险号、(xii) 驾驶执照号、(xiii) 护照号、(xiv) 与在线游戏服务相关联的用户ID、或(xv) 政府实体发布的ID。

[0173] 在一些实施例中,可信身份模块312可以被配置为通过使用不同的标识来验证居住在具有不同法院系统的不同区域中的不同用户。例如,可信身份模块312可以被配置为使用与第一用户相关联的第一法院系统承认的第一组标识中的至少一个来验证第一用户的身份,以及使用与第二用户相关联的第二法院系统承认的第二组标识中的至少一个来验证第二用户的身份,其中,第一用户和第二用户居住在具有不同法院系统的不同区域中。

[0174] 在一些实施例中,可信计算模块314可以包括具有TEE的一个或多个数据处理器,该TEE与一个或多个数据处理器的操作系统隔离并且被配置为为一个或多个数据处理器中执行的代码和加载的数据提供增强的机密性和完整性。

[0175] 在一些实施例中,可信计算模块314可以被配置为根据隐私法律记录与用户相关联的信息。例如,可信计算模块314可以生成记录的哈希值,并将包括所述记录和所述哈希值的区块添加到存储与用户1002相关联的记录的区块链1010。

[0176] 在一些实施例中,法律文档工具306可以被配置为执行多个步骤以处理用于进行服务的信息,并且对于多个步骤中的至少一些步骤中的每个步骤,法律文档工具306可以被配置为调用可信计算模块以处理区块链数据,从而更新区块链以记录包括可信时间模块生成的经验证时间戳和/或可信身份模块确定的经验证身份的信息,其中,所述经验证时间戳表示在执行服务的信息处理中的事件的时间,所述经验证身份表示用户的身份。

[0177] 在一些实施例中,可信计算模块314可以被配置为响应于对与法律文档相关联的经验证记录的请求,提供由法律文档工具306执行的步骤/操作的经验证记录。可信计算模块314还可以提供与由法律文档306执行的步骤/操作中的每个步骤/操作相关联的经验证时间戳、经验证身份和/或计算结果。

[0178] 在一些实施例中,法律文档工具306可以允许用户根据法律文档处理的法律要求填写电子法律文档。在一些实施例中,法律文档工具306可以获得并记录由法律文档工具306执行的、针对法律文档处理的多个步骤中的每个步骤的经验证时间戳、经验证身份和/或计算结果。法律文档工具306可以从可信时间模块310获得经验证时间戳,从可信身份模块312获得经验证身份,以及从可信计算模块314获得计算结果。

[0179] 在一些实施例中,法律文档工具306可以包括被配置为在可信执行环境中执行,并记录由法律文档工具306执行的步骤以及与所述步骤的每个步骤相关联的经验证时间戳、经验证身份和/或计算结果的可信组件(未示出)。在一些实施例中,可信组件可以包括被配置为基于哈希算法生成表示由法律文档工具执行的步骤的数据的哈希值的哈希计算组件。

[0180] 在一些实施例中,法律文档工具306可以被配置为通过与可信时间模块310、可信身份模块312或可信计算模块314相关联的相应的API(例如,API 810、812和814)调用可信

时间模块310、可信身份模块312或可信计算模块314的功能。在一些实施例中,API 810、812和814可以包括任何合适的API,诸如REST网络API(或RESTful API)或基于SOAP的网络API等。

[0181] 在一些实施例中,法律文档工具306可以在接收到从与基于区块链应用相关联的用户的账户发起的、用于提供服务的请求时,调用可信身份模块312以验证用户(例如,用户1002)的身份。法律文档工具306可以进一步识别用于提供服务的多个步骤中填写和提交的一个或多个电子表格。

[0182] 在一些实施例中,在多个步骤中的每个步骤,法律文档工具306可以调用可信时间模块310以生成执行该步骤的时间,并基于执行该步骤的时间以及此时电子表格上的数字内容来生成唯一标识(ID)。法律文档工具306可以进一步调用可信计算模块以在区块链上记录唯一ID、时间和数字内容。然后,法律文档工具306可以通过更改与数字内容相关联的一个或多个属性来表示唯一ID,从而将该唯一ID嵌入此时的数字内容中,其中,该嵌入产生能够基于该唯一ID从区块链检索所述时间和数字内容的嵌入信息的数字内容。法律文档工具306可以进一步调用可信计算模块以将嵌入信息的数字内容记录到区块链。

[0183] 图11是示出可根据本文实施例执行的处理1100的示例的流程图。处理1100可以由一个或多个区块链节点或通信地耦接到一个或多个区块链节点的计算设备来执行。为了清楚地呈现,以下描述结合本文中的其他附图总体地描述了处理1100。然而,应当理解,处理1100可以例如通过任何系统、环境、软件和硬件,或者系统、环境、软件和硬件的组合来适当地执行。在一些实施例中,处理1100的各个步骤可以并行、组合、循环或以任何顺序运行。

[0184] 在1102,接收对服务的请求。该服务可以是由政府机构提供的公共服务、由业务服务提供者提供的业务服务。例如,该服务可以是驾驶执照续期服务、税务登记服务、结婚登记服务、银行开户服务、居住证服务,公寓租赁服务等。在一些实施例中,用户可以通过从法律文档工具306的用户账户或承载法律文档工具306的另一基于区块链应用访问可信平台300的法律文档工具306,发起对服务的请求。例如,用户可以在用户的客户终端上打开法律文档工具306并登录账户。然后可以在用户的客户终端上显示可用的服务,并且用户可以通过选择所需的服务发起请求。

[0185] 在一些实施例中,可以从与法律文档工具306相关联的服务提供者的账户发起用于处理用户的服务请求的第二请求。用以处理用户的请求的第二请求可以是检查用户的文书工作,对用户的文书工作做出决定,对用户的签名进行背书,在检查用户的文书工作之后发送补充文档请求等。

[0186] 在1104,验证身份。身份可以是用户的或服务提供者代表的身份。在一些实施例中,身份可以被包括在对服务的请求中。

[0187] 在一些实施例中,法律文档工具306调用可信身份模块312以验证用户或服务提供者代表的身份。在一些实施例中,用户或代表可以使用生物特征信息进行注册。当用户或代表访问法律文档工具306时,可以要求用户或代表使用指纹、语音、虹膜或面部识别来验证他/她的身份。在通过传感器输入相应的生物特征信息之后,可信身份模块312可以将生物特征信息与存储在存储器中的注册信息进行匹配,以验证用户或代表是否被授权使用法律文档工具306。

[0188] 在1106,识别将被填写和提交的、用以提供服务的一个或多个电子表格。一个或多

个电子表格可以是服务提供者提供服务所需的数字文书。例如,电子表格可以是申请表格、服务协议、会员续期表格、租赁协议、采购订单等。电子表格可以包括一个或多个在线页面。

[0189] 在1108,确定是否存在待在电子表格上执行的附加步骤。在一些实施例中,填写电子表格可以包括多个步骤。例如,填写租赁协议可以包括签署租赁协议的每一页。签署每个签名或首字母可以是填写协议的单独步骤。这些步骤可以由用户和/或服务提供者执行。例如,用户可以在一个步骤中在电子表格的页面上签名,而在另一步骤中,服务提供者可以在同一页面上签名以对该用户的签名进行背书。在一些实施例中,用户和服务提供者都可以访问法律文档工具306以交互地执行步骤,例如,在一方可以背书或会签之前,另一方可以保持登录状态以等待该方完成他/她的签名。在一些实施例中,用户和服务提供者可以分别登录以执行他们自己的信息文档处理步骤。如果存在要执行的附加步骤,则处理1100进行到1110。否则,处理1100进行到1116。

[0190] 在1110,基于执行步骤的时间和此时电子表格上的数字内容来生成唯一ID。该唯一ID可用于唯一地标识用户。在一些实施例中,该唯一ID可以包括利用用户的私钥数字签名的该用户的身份信息。然后,可以通过利用对应于该用户的公钥对数字签名进行解密来识别该用户,以及通过将该解密的信息与记录在区块链中的该用户的可信身份进行比较来验证该用户。在一些实施例中,可以基于时间和此时用户填写在电子表格上的数字内容来生成唯一ID。在一些实施例中,可以基于时间和电子表格来生成唯一ID。

[0191] 在一些实施例中,该唯一ID可以嵌入在用户填写的数字内容中。在一些实施例中,可以基于执行第二步骤的时间和此时服务提供者填写在电子表格上的数字内容来生成第二唯一ID。该第二唯一ID可以嵌入在服务提供者填写的数字内容中。

[0192] 在一些实施例中,包括执行步骤的时间以及此时电子表格上的数字内容的至少部分内容可以用于生成唯一ID,例如通过基于部分内容生成哈希值。在一些实施例中,用于生成唯一ID的内容还包括用户或服务提供者的身份。

[0193] 在一些实施例中,可以对唯一ID进行加密或哈希处理以增强鲁棒性和安全性。例如,可以使用用户或服务提供者的公钥基于公钥加密法来执行加密。在一些实施例中,还可以基于诸如Arnold加扰加密的加密方案来执行加密,以适应所使用的嵌入技术。通过执行加密,如果攻击者不知道加密方案或加密密钥,即使攻击者提取出数字水印,也不能解密出相关联的唯一ID。

[0194] 在1112,唯一ID、时间和数字内容被记录在区块链上。在一些实施例中,唯一ID、时间和数字内容可以以键值对的形式作为交易记录在区块链上,其中键是唯一ID,并且值包括时间和数字内容。然后,可以使用唯一ID来检索包括时间和数字内容的值。在一些实施例中,区块链网络可采用诸如默克尔帕特里夏树或固定深度默克尔树的内容寻址树结构。在一些实施例中,与可信平台相关联的区块链网络中的每个区块链节点可以存储区块数据或状态数据的一部分。例如,与存储唯一ID、时间和数字内容的全节点相比,区块链节点可以是仅存储唯一ID和时间而不存储数字内容的轻节点。在一些实施例中,区块链网络可包括存储历史状态数据的一个或多个共享存储节点,而其他常规区块链节点仅存储当前状态数据以节省存储空间。

[0195] 在1114,唯一ID被嵌入在数字内容中。在一些实施例中,每个步骤对应于电子表格的页面。可以在电子表格的每一页中嵌入唯一的ID。在一些实施例中,可以通过更改与数字

内容相关联的一个或多个属性来表示唯一ID,将唯一ID嵌入数字内容中,其中,该嵌入产生能够基于该唯一ID从区块链检索所述时间和数字内容的嵌入信息的数字内容。在一些实施例中,唯一ID可以被不可见地嵌入。如果这样的添加对肉眼不明显或不可见,则可以认为该嵌入的唯一ID是不可见的。换句话说,如果在嵌入唯一ID之前和嵌入唯一ID之后数字内容之间的视觉差异对于肉眼不明显,则可以认为该唯一ID是不可见的。唯一ID可以嵌入在数字内容、数字内容的前景或数字内容的背景中。数字内容的前景可以是附着或集成到显示数字内容的平台的膜或屏幕。数字内容的前景也可以是包含唯一ID的层,所述唯一ID被配置为不被查看应用所呈现。数字内容的背景可以是包含在显示器上呈现的数字内容的电子文件的视觉表示的背景。

[0196] 可以基于数字水印处理来执行数字内容的不可见嵌入。数字水印处理是一种使用数据载体嵌入唯一ID的技术。数据载体可以包括文本、图像、或电子媒介。唯一ID可以作为不可见的数字水印嵌入数据载体中。当对数字内容进行查询时,可以从数据载体中提取唯一ID以检索与该唯一ID对应的数字内容。

[0197] 数字水印处理技术可以包括背景亮度掩蔽、照度掩蔽、纹理掩蔽、空间掩蔽和频率掩蔽。不同的技术可以基于不同的数字水印处理算法。在一些实施例中,数字水印嵌入可以基于人类视觉系统(HVS)特性以实现视觉不可感知性或不可见性。例如,人眼对低强度像素的变化比高强度像素的变化更敏感。在照度掩蔽中,可以扫描数字内容的像素以识别具有高强度水平的像素。高强度像素可用于嵌入数字水印。人眼难以察觉对高强度像素进行的修改,使得可以认为数字水印是不可见地嵌入的。使用照度掩蔽,数字水印可以嵌入整个数字内容或数字内容的一部分中。例如,如果数字内容是文本内容,则数字水印可以嵌入字、单词、句子或一直到整个文本内容中。

[0198] 作为另一示例,在纹理掩蔽中,纹理越复杂,人眼就越难以辨别纹理的变化。因此,数字水印可以嵌入到具有更复杂的纹理的数字图像的一部分或数字内容的背景中,以使人眼不易察觉。

[0199] 作为又一示例,可以通过基于诸如离散余弦变换(DCT)、离散小波变换(DWT)或Arnold变换的数学变换将数字内容转换为频域系数,基于频率掩蔽来执行数字水印处理。在频率掩蔽中,通常根据水印信息修改中频或低频系数。这些频率范围对原始内容的呈现影响较小。数字水印(即,唯一ID)可以是字符串的形式。字符串可以转换为单个二进制字符串。可以嵌入每个比特(bit)以根据所使用的变换技术调整低频系数。在频率掩蔽中,数字水印可以被分散到整个数字内容,这可以增加鲁棒性和不可见性。用于执行数字水印处理的其他示例性数学变换可以包括DWT和奇异值分解(DWT-SVD)、最低有效位(LSB)或高度不可检测的隐写(HUGO)。

[0200] 在一些实施例中,可以使用一种以上的数字水印处理技术将多层数字水印嵌入到数据载体中。在这种情况下,还可以生成数字水印层的索引并将其嵌入数据载体中。该索引可用于从数据载体中更容易地提取数字水印。在一些实施例中,在嵌入到数据载体之前,可以将唯一ID随机化或与随机信号混合。

[0201] 在一些示例中,数字内容可以是文本内容。如果嵌入的唯一ID不会实质性地改变内容,则可以将其视为不可见。如果嵌入的信息不改变文本的含义,则可以认为内容没有实质性改变。例如,原始文本是“he becomes amonster after seven years”,嵌入信息的文

本是“he has become a ‘monster’ after seven years”。由于文本的含义保持不变,因此添加的文本中嵌入的信息不会被视为对原始文本进行了实质性改变。在该示例中,根据本文描述的技术,唯一ID可以嵌入引号中,或者助动词“has”中。在一些实施例中,唯一ID可以嵌入空格或例如冠词、介词、连词和助动词的功能词中,它们通常不会改变文本内容的实质含义。

[0202] 在一些实施例中,可以使用多个唯一ID来跟踪文本内容的更新。例如,可以基于记录在区块链上的对应于一个或多个数字内容更新的时间戳来生成一个或多个唯一ID。当执行内容更新并将其记录在区块链上时,包括相应时间戳的唯一ID可以嵌入在更新内容的至少一部分中。从数字内容中提取的唯一ID中的时间戳可以形成数字内容的创作和更新历史的时间线。该时间线可以用作内容开发过程的证据,并与区块链上记录的更新历史进行比较,以认证文本内容的作者身份。

[0203] 在一些实施例中,唯一ID可以嵌入在文本或图像内容的特征信息中。示例性特征信息可以包括文本或图像的颜色、亮度和透明度。例如,可以基于红绿蓝 (RGB) 颜色模型对文本或图像颜色进行编码。可嵌入唯一ID以略微改变RGB值组合,肉眼对这种改变无法察觉。作为另一示例,唯一ID可以嵌入YCbCr格式的文本或图像中,其中Y表示亮度信号、Cb表示色度蓝信号、Cr表示色度红信号。亮度信号对信息嵌入相对不敏感,其可以优选地用于不可见地嵌入唯一ID。

[0204] 在一些实施例中,唯一ID可以嵌入文本内容的标点符号中。例如,在文本“after seven years, he becomes a ‘monster’,”中,唯一ID可以嵌入逗号和引号的编码中。

[0205] 在一些实施例中,唯一ID可以嵌入由文本内容使用的字体中。可以使用例如UTF-8的统一码(Unicode)对字体进行编码。UTF-8基于可变宽度字符编码,使用一到四个8位字节。在某些位中嵌入唯一ID可能会略微改变像素位置、大小、角度、字体形状或标点符号,这种改变对肉眼不可见。例如,可以用冗余来编码文本字体和标点符号的像素。通常将冗余添加到像素以用于数据通信中的错误检查。诸如校验位的冗余可用于检查接收方端的数据完整性。如果校验位在到达接收方时与承载像素的其余信息不一致,则接收方可以要求发送方重新发送内容。唯一ID可以随机地嵌入冗余像素中或嵌入固定位置的冗余像素中。应该理解,唯一ID也可以不可见地嵌入字体或标点符号的其他隐藏特征中。

[0206] 在一些实施例中,唯一ID可以嵌入在数字内容中的或包含数字内容的表单或表格中。这些实施例特别适用于在在线表单或表格中插入的文本或图像的权利认证。例如,在线表单可以是在网页的超文本标记语言 (HTML) 定义中定义的表单 (例如通过使用“<form>”标签) 并由显示该网页的浏览器程序呈现。类似地,在线表格可以是在网页的超文本标记语言 (HTML) 定义中定义的表格 (例如通过使用“<table>”标签) 并由显示该网页的浏览器程序呈现。唯一ID可以不可见地嵌入与颜色、阴影、单元格大小或表单或表格的其他属性相关联的值中。

[0207] 在一些情况下,唯一ID可以嵌入可用于显示或发布数字内容的电子媒介中。例如,唯一ID可以嵌入网页或例如MICROSOFT WORD、POWERPOINT或ADOBE PDF的电子文件的背景纹理中。

[0208] 在1116,将嵌入信息的数字内容记录到区块链。在一些实施例中,可以建立唯一ID和嵌入信息的数字内容之间的相关性,并且可以基于查询唯一ID来从区块链检索该嵌入信

息的数字内容。

[0209] 图12是示出根据本文实施例的用于提供争议解决方案的系统1200的示例的图。系统1200实现了基于区块链网络的争议解决方案。总体地,系统1200允许两个或更多个争议方以方便的方式从多个争议解决方案提供者(例如,争议调解员)处找到一个或多个潜在解决方案。

[0210] 作为示例,系统1200包括客户终端1204a和1204b(分别由用户1202a和1202b使用),基于区块链的可信平台300和区块链网络1216。系统1200与几个争议解决方案提供者1206a-1206m通信。如图所示,基于区块链的可信平台300包括争议解决工具304,API 810、812和814,可信时间模块310、可信身份模块312和可信计算模块314。注意,基于区块链的可信平台300被示出为包含了争议解决工具304,仅旨在说明。基于区块链的可信平台300可以包括任何合适数量的工具,例如传票送达工具(例如,图3的传票送达工具302)、法律文档工具(例如,法律文档工具306)和判决执行工具(例如,判决执行工具308)等。在一些实施例中,可信平台300与区块链网络1216中的节点1214之一相关联,其中区块链(例如区块链1210)是跨区块链网络1216复制的。

[0211] 在一个示例中,用户1202a可以使用客户终端1204a来向区块链网络1216发送网络服务请求(例如,解决法律争议的请求)。与区块链网络1216中的区块链网络节点1214相关联的可信平台300可以处理并满足网络服务请求(例如,经由客户终端1204b将争议解决方案提供给用户1202a)。作为另一示例,用户1202a和用户1202b可以共同向可信平台300提交涉及用户1202a和用户1202b的法律争议。可信平台300可以邀请多个争议解决方案提供者1206a-1206m给出争议解决方案,并且识别用户1202a和用户1202b都同意的一个或多个争议解决方案。

[0212] 客户终端1204a和1204b可以包括,例如,被编程为执行本文所描述的方法的任何合适的计算机、模块、服务器或计算元件。在一些实施例中,客户终端1204a和1204b可以包括用于提供客户终端1204a和1204b的各种功能的网络浏览器和软件应用。

[0213] 在一些实施例中,争议解决工具304可以为至少第一方(例如,用户1202a)和第三方(例如,用户1202b)之间的争议提供一个或多个潜在解决方案。在一些实施例中,争议解决工具304可以调用可信身份模块(例如,可信身份模块312)以验证第一方的身份,验证第三方的身份以及验证多个争议解决方案提供者(例如,争议解决方案提供者1206a-1206m)的身份。争议解决工具304可以进一步将与争议有关的信息发送给多个争议解决方案提供者。

[0214] 在一些实施例中,争议解决工具304可以从多个争议解决方案提供者1206a-1206m接收针对该争议的潜在解决方案,并将所述潜在解决方案发送给第一方和第三方。在一些实施例中,争议解决工具304可以从第一方和第三方接收回应,并且基于该回应来确定双方是否接受至少一个解决方案。例如,争议解决工具304可以从第一方接收第一组潜在争议解决方案,并从第三方接收第二组潜在争议解决方案。争议解决工具304可以确定第一组和第二组是否存在至少一个共同的争议解决方案。如果确定不存在共同的争议解决方案,则争议解决工具304可以确定无一潜在解决方案是第一方和第三方均可接受的。

[0215] 在一些实施例中,争议解决工具304可以更新区块链(例如,区块链1210)以记录与由争议解决工具304提供的服务相关联的数据。例如,争议解决工具304可以更新区块链

1210以记录表示双方1202a和1202b之间的争议的数据以及由争议解决方案提供者1206a-1206m提供的潜在解决方案的数据。争议解决工具304可以更新区块链1210以记录表示争议双方1202a和1202b的身份的数据以及争议解决方案提供者1206a-1206m的身份的数据。

[0216] 在一些实施例中,争议解决工具304可以更新区块链1210以记录表示第一时间戳的数据和表示第二时间戳的数据,其中,该第一时间戳指示关于争议的信息何时被发送到争议解决方案提供者1206a-1206m,第二时间戳指示每一个争议服务提供者1206a-1206m何时提供了潜在争议解决方案。在一些实施例中,争议解决工具304可以更新区块链1210以记录表示第一时间戳的数据、表示第二时间戳的数据、表示第三时间戳的数据、表示第四时间戳的数据;其中,该第一时间戳指示潜在争议解决方案何时被发送给第一方1202a,第二时间戳指示潜在争议解决方案何时被发送给第二方1202b,第三时间戳指示第一方1202a何时提供对潜在争议解决方案的回应,第四时间戳指示第二方1202b何时提供对潜在争议解决方案的回应。

[0217] 在一些实施例中,争议解决工具304可以从第一方1202a接收指示第一方1202a可以接受至少第一组潜在争议解决方案的第一回应,并且从第二方1202b接收指示第二方1202b可以接受至少第二组潜在争议解决方案的第二回应。争议解决工具304可以基于第一回应和第二回应确定是否存在至少一个共同的争议解决方案。例如,争议解决工具304可以基于第一方1202a和第二方1202b两者都可接受的一个或多个潜在解决方案来确定至少一个最终潜在解决方案。

[0218] 在一些实施例中,争议解决工具304可以向争议解决方案提供者1206a-1206m中促成了第一方1202a和第二方1202b都可接受的至少一个最终潜在解决方案的至少一个争议解决方案提供者提供资产。

[0219] 在一些实施例中,争议解决工具304可以被配置为通过与可信时间模块310、可信身份模块312或可信计算模块314相关联的相应的API(例如,API 810、812和814)调用可信时间模块310、可信身份模块312或可信计算模块314的功能。在一些实施例中,API 810、812和814可以包括任何合适的API,诸如REST网络API(或RESTful API)或基于SOAP的网络API等。

[0220] 图13是示出可根据本文实施例执行的用于实施争议解决方案的处理1300的示例的流程图。为方便起见,处理1300将被描述为由位于一个或多个位置并根据本文被适当地编程的一个或多个计算机的系统执行。例如,被适当地编程的诸如图12的系统1200的分布式系统可以执行处理1300。

[0221] 在1302,在基于区块链应用(例如,争议解决工具304)处接收用于解决至少第一方(例如,用户1202a)和第二方(例如,用户1202b)之间的争议的请求。在一些实施例中,解决争议的请求可以包括虚拟资产。在一些实施例中,虚拟资产是数字资产的表示,其可以被定义为交换媒介或在诸如金融贸易环境的特定环境中具有价值的财产。在一些实施例中,可以将虚拟资产提供给争议解决方案提供者(例如,争议解决方案提供者1206a-1206m)作为奖励以激励争议解决方案提供者研究争议并提出明智的争议解决方案。

[0222] 在一些实施例中,基于区块链应用可以从第一方接收用以解决争议的第一请求。第一请求可以包括具有第一价值的第一虚拟资产。基于区块链应用可以从第二方接收用以解决争议的第二请求。第二请求可以包括具有第二价值的第二虚拟资产。在一些实施例中,

基于区块链应用可以基于第一虚拟资产和第二虚拟资产中价值较高的一个虚拟资产来确定虚拟资产。例如,如果第一虚拟资产的价值比第二虚拟资产的价值高,则可以将第一虚拟资产确定为虚拟资产。

[0223] 在一些实施例中,基于区块链应用可以将虚拟资产存储为存款。在一些实施例中,基于区块链应用可以分别从与第一方关联的第一账户中移除虚拟资产,并且从与第二方关联的第二账户中移除虚拟资产,以及将从第一个账户和第二个账户中移除的虚拟资产存储在区块链上。继续以上示例,如果第一虚拟资产的价值比第二虚拟资产的价值高,则可以将第一虚拟资产确定为最终虚拟资产,并且可以从与第一方关联的第一账户中取出第一虚拟资产。也可以从与第二方关联的第二账户中取出第一虚拟资产。基于区块链应用可以将两块第一虚拟资产存储为最终虚拟资产,以奖励争议解决方案提供者。

[0224] 在步骤1304,确定第一方和第二方是否是基于区块链应用的注册用户。在一些实施例中,确定基于将第一身份与第一方的记录在区块链上的注册信息中包含的身份进行匹配,以及将第二身份与第二方的记录在区块链上的注册信息中包含的身份进行匹配。在一些实施例中,基于区块链应用可以调用可信身份模块(例如,可信身份模块312)以验证第一方的身份和第二方的身份。基于区块链应用可以进一步调用可信身份模块,以验证多个争议解决方案提供者(例如,争议解决方案提供者1206a-1206m)的身份。

[0225] 在一些实施例中,基于区块链应用可以调用可信计算模块(例如,可信计算模块314)以记录表示争议各方的身份的数据和表示争议解决方案提供者的身份的数据。

[0226] 如果确定第一方和第二方不是基于区块链应用的注册用户,则该处理进行到步骤1306,其中通知被发送到第一方和第二方,以通知:第一方和第二方不是注册用户。如果确定第一方和第二方是基于区块链应用的注册用户,则处理进行到步骤1308。

[0227] 在1308,在区块链上记录接收到请求的时间。在一些实施例中,基于区块链应用可以调用可信时间模块(例如,可信时间模块310)以记录指示何时从第一方接收到第一请求的时间戳和指示何时从第二方接收到第二请求的时间戳。在一些实施例中,基于区块链应用可以调用可信计算模块(例如,可信计算模块314)以记录表示双方之间的争议的数据。

[0228] 在一些实施例中,基于区块链应用可以将与争议有关的信息发送给多个争议解决方案提供者。在一些实施例中,基于区块链应用300可以调用可信时间模块310以记录表示指示关于该争议的信息何时被发送到争议解决方案提供者的时间戳的数据。

[0229] 在1310,从在基于区块链应用(例如,争议解决工具304)上注册的一个或多个争议解决方案提供者接收一个或多个潜在争议解决方案。在一些实施例中,可以请求在预定时间窗内接收一个或多个潜在争议解决方案。在一些实施例中,基于区块链应用(例如,304)可以调用可信时间模块310以记录表示指示每个争议解决方案提供者何时提供潜在争议解决方案的时间戳的数据。在一些实施例中,基于区块链应用可以调用可信计算模块314以记录表示争议解决方案提供者提供的潜在解决方案的数据。

[0230] 在一些实施例中,基于区块链应用可以将潜在解决方案发送给第一方和第二方。在一些实施例中,基于区块链应用可以调用可信时间模块310以记录表示指示潜在争议解决方案何时被发送到第一方的时间戳的数据和表示指示潜在争议解决方案何时被发送到第二方的时间戳的数据。

[0231] 在1312,从第一方接收第一选择、从第二方接收第二选择。在一些实施例中,第一

选择包括第一组一个或多个潜在争议解决方案,第二选择包括第二组一个或多个潜在争议解决方案。在一些实施例中,基于区块链应用可以调用可信计算模块314以记录表示来自第一方的第一选择的数据和表示来自第二方的第二选择的数据。

[0232] 在1314,将接收到第一选择的时间和接收到第二选择的时间记录在区块链上。例如,基于区块链应用可以调用可信时间模块310以记录表示指示第一方何时提供了潜在争议解决方案的第一选择的时间戳的数据,以及表示指示第二方何时提供了潜在争议解决方案的第二选择的时间戳的数据。

[0233] 在1316,确定在第一组一个或多个潜在争议解决方案与第二组一个或多个潜在争议解决方案之间是否存在至少一个共同的潜在争议解决方案。

[0234] 如果确定在第一组一个或多个潜在争议解决方案和第二组一个或多个潜在争议解决方案中存在至少一个共同的潜在争议解决方案,则该处理进行到步骤1318。如果确定第一组一个或多个潜在争议解决方案与第二组一个或多个潜在争议解决方案之间没有共同的潜在争议解决方案,则基于区块链应用可以确定无一潜在争议解决方案是第一方和第三方均可以接受的,处理进行到步骤1320。

[0235] 在1318,将虚拟资产发送到提供该共同的潜在争议解决方案的至少一个争议解决方案提供者。例如,可以向促成了第一方和第三方都可接受的至少一个共同的潜在解决方案的至少一个争议解决方案提供者提供虚拟资产。

[0236] 在1320,如果确定在第一组一个或多个潜在争议解决方案和第三组一个或多个潜在解决方案之间没有共同的潜在解决方案,则可从法定授权实体接收争议解决方案。在一些实施例中,法定授权实体不同于争议解决方案提供者。

[0237] 在一些实施例中,分别在预定时间窗内从第一方接收第一选择和从第三方接收第二选择。

[0238] 在一些实施例中,还确定接收的争议解决方案是否与第一组一个或多个争议解决方案中的争议解决方案和第三组一个或多个争议解决方案中的争议解决方案匹配。如果确定争议解决方案与第一方选择的第一组争议解决方案中的争议解决方案最接近匹配,则可以将第三方的第二账户中取出的虚拟资产发送到争议解决方案提供者,该提供者提供了第一组争议解决方案中的争议解决方案。如果确定争议解决方案与第三方选择的第三组争议解决方案中的争议解决方案最接近匹配,则可以将从第一方的第一账户取出的虚拟资产发送给争议解决方案提供者,该提供者提供了第三组争议解决方案中的争议解决方案。

[0239] 图14是示出根据本文实施例的用于判决执行的系统1400的示例的图。系统1400实现了基于区块链网络执行法院判决的处理。通常,系统1400提供了一种执行法院判决的方法,其中每个判决指定债务人、债权人以及债务人欠债权人的判决金额。

[0240] 作为示例,系统1400包括债务人1402、债权人1404、债务人1406的一个或多个支付账户、判决金额1408、债权人1410的支付账户、法院判决1412、基于区块链的可信平台300和区块链网络1416。如图所示,基于区块链的可信平台300包括法律文档工具306,API 810、812和814,可信时间模块310、可信身份模块312和可信计算模块314。注意,基于区块链的可信平台300被示出为包含了判决执行工具308,仅旨在说明。基于区块链的可信平台300可以包括任何合适数量的工具,例如传票送达工具(例如图3的传票送达工具302)、争议解决工具(例如,争议解决工具304)和法律文档工具(例如,法律文档工具306)等。在一些实施例

中,可信平台300与区块链网络1416中的节点1414之一相关联,其中区块链(例如区块链1410)是跨区块链网络1416复制的。

[0241] 在一个示例中,在区块链网络1416中的区块链网络节点1414上实现的基于区块链的可信平台300可以处理并执行法院判决1412。然后可以将判决金额1408从债务人1406的一个或多个支付账户转账到债权人1410的支付账户。

[0242] 在一些实施例中,判决执行工具308可以被配置为采用SM2算法,该SM2算法是基于椭圆曲线的公钥加密算法,以对数据通信进行加密并验证身份。在一些实施例中,可以为由判决执行工具308记录的内容指定访问级别。某些记录的内容只能由具有指定访问级别的人员访问。

[0243] 在一些实施例中,可信时间模块310可以被配置为基于(i)国家标准时间信息和/或(ii)从全球定位系统获得的时间信息来生成时间戳。在一些实施例中,区块链网络可以从单个源获得时间,使得区块链网络中的所有区块链节点可以被同步为同一时间。

[0244] 例如,可信时间模块310可以被配置为使用与第一债务人或债权人相关联的第一法院系统承认的第一标准时间来生成与第一债务人或债权人相关联的时间戳,以及使用与第二债务人或债权人相关联的第二法院系统承认的第二标准时间来生成与第二债务人或债权人相关联的时间戳,其中,第一债务人或债权人与第二债务人或债权人居住在具有不同法院系统的不同区域中。

[0245] 在一些实施例中,可信身份模块312可以被配置为基于与债务人或债权人相关联的一个或多个标识来验证债务人或债权人的身份,所述标识包括以下中的至少一个:(i) 手机号码、(ii) 信用卡号、(iii) 与在线支付系统关联的用户ID、(iv) 与在线购物账户关联的用户ID、(v) 与音乐流或下载账户相关联的用户ID、(vi) 与电影流或下载账户相关联的用户ID、(vii) 与消息传送或聊天账户相关联的用户ID、(viii) 与在线银行账户相关联的用户ID、(ix) 与约车服务相关联的用户ID、(x) 与在线食品订购服务相关联的用户ID、(xi) 社会保险号、(xii) 驾驶执照号、(xiii) 护照号、(xiv) 与在线游戏服务相关联的用户ID、或(xv) 政府实体发布的ID。

[0246] 在一些实施例中,可信身份模块312可以被配置为使用与第一债务人或债权人相关联的第一法院系统承认的第一组标识中的至少一个来验证第一债务人或债权人的身份,以及使用与第二债务人或债权人相关联的第二法院系统承认的第二组标识中的至少一个来验证第二债务人或债权人的身份,其中,第一债务人或债权人与第二债务人或债权人居住在具有不同法院系统的不同区域中。

[0247] 在一些实施例中,可信计算模块314包括具有TEE的一个或多个数据处理器,该TEE与一个或多个数据处理器操作系统隔离并且被配置为为一个或多个数据处理器中执行的代码和加载的数据提供增强的机密性和完整性。

[0248] 在一些实施例中,可信计算模块314可以被配置为根据隐私法律记录与债务人和/或债权人相关联的信息。

[0249] 在一些实施例中,基于区块链的判决执行工具308可以被配置为执行法院判决,其中每个判决指定债务人(例如,债务人1402)、债权人(例如,债权人1404)以及债务人欠债权人的判决金额(例如,判决金额1408)。判决执行工具308可以进一步调用可信时间模块以生成第一经验证时间戳,该第一经验证时间戳表示该判决执行工具接收到法院判决的时间。

[0250] 在一些实施例中,判决执行工具308可以被配置为识别与债务人相关联的一种或多种资产。判决执行工具308还可以从与债务人相关联的一种或多种资产中收集至少一部分判决金额。判决执行工具308可以进一步被配置为将所收集的资产发送给债权人。

[0251] 在一些实施例中,判决执行工具308可以被配置为确定与债务人相关联的一个或多个支付账户,将法院判决发送给管理与债务人相关联的一个或多个支付账户的一个或多个金融机构,并请求所述一个或多个金融机构从与债务人相关联的支付账户中收集至少一部分判决金额。

[0252] 判决执行工具308可以进一步调用可信时间模块以生成第二经验证时间戳,该第二经验证时间戳表示收集到的资产何时被发送给债权人。判决执行工具308还可以调用可信计算模块来处理区块链数据以在区块链中添加记录,其中该记录包括与债务人和债权人的身份、第一经验证时间戳和第二经验证时间戳以及从债务人收集到的并发送给债权人的资产的金额有关的信息。

[0253] 在一些实施例中,判决执行工具308可以被配置为执行多个步骤以执行法院判决,并且对于多个步骤中的至少一些步骤中的每个步骤,判决执行工具308可以被配置为调用可信计算模块来处理区块链数据以更新区块链,从而记录包括可信时间模块生成的经验证时间戳、和/或可信身份模块确定的经验证身份的信息,其中,所述经验证时间戳表示执行法院判决中的事件的时间,所述经验证身份代表债权人或债务人的身份。

[0254] 在一些实施例中,判决执行工具308可以被配置为处理区块链中的数据以提供与执行判决的多个步骤相关联的经验证记录。

[0255] 在一些实施例中,判决执行工具308包括被配置为在TEE中执行并且记录与由判决执行工具308执行的至少一些步骤相关联的数据的可信组件。

[0256] 在一些实施例中,可信组件包含被配置为基于哈希算法生成表示与由判决执行工具308执行的至少一些步骤相关联的数据的哈希值的哈希计算组件。

[0257] 在一些实施例中,基于区块链的判决执行工具被配置为通过与可信时间模块、可信身份模块或可信计算模块相关联的相应的应用编程接口(API)调用可信时间模块、可信身份模块或可信计算模块的功能。

[0258] 在一些实施例中,基于区块链的判决执行工具308可以包括客户端组件和服务器组件,客户端组件可以被配置为在债务人或债权人的客户终端处执行,并且服务器组件可以被配置为在系统的计算机服务器处执行。

[0259] 在一些实施例中,判决执行工具308可以被配置为使债务人能够访问区块链数据以验证从与债务人相关联的一个或多个资产中收集的金额与法院判决相一致。

[0260] 在一些实施例中,判决执行工具308可以被配置为使债权人能够访问区块链数据以验证已经从与债务人相关联的一个或多个资产中收集了金额。

[0261] 在一些实施例中,判决执行工具308可以被配置为使法院的代表能够访问区块链数据以验证判决执行进度。

[0262] 图15是示出了可根据本文实施例执行的处理1500的示例的流程图。处理1500可以由一个或多个区块链节点或通信地耦接到一个或多个区块链节点的计算设备来执行。为了清楚地呈现,以下描述结合本文中的其他附图总体地描述了处理1500。然而,应当理解,处理1500可以例如通过任何系统、环境、软件和硬件,或者系统、环境、软件和硬件的组合来适

当地执行。在一些实施例中,处理1500的各个步骤可以并行、组合、循环或以任何顺序运行。

[0263] 在1502,接收用以收集法院命令中发布的货币裁定的请求。在一些实施例中,该请求与基于区块链应用的账户相关联。在一些实施例中,请求可以包括与账户相关联的身份。货币裁定可以是例如现金、资金、股票、债券、外币或其他类型的资产。在一些实施例中,该请求可以由法院或债权人发起。

[0264] 在一些实施例中,该请求是第一请求,并且该账户是第一账户。在接收第一请求之前,可以接收与基于区块链应用的第二账户相关联的第二请求,该第二请求用于记录法院命令,其中第二请求包括与第二账户相关联的身份。基于可信身份模块,可以基于与第二账户相关联的身份和记录在区块链上的第二账户的注册信息来确定第二账户与法院相关联。可以调用可信计算模块以将命令在区块链上记录为命令的哈希值。可信时间模块可以记录表示命令被记录在区块链上的时间的第三经验证时间戳。

[0265] 在1504,确定命令是否真实。在一些实施例中,可以由可信身份模块(例如,可信身份模块312)基于与记录在区块链上的命令相关联的哈希值进行匹配来确定。

[0266] 在1506,在区块链上记录表示接收到请求的时间的第一经验证时间戳。在一些实施例中,可信时间模块(例如,可信时间模块310)记录第一经验证时间戳。

[0267] 在1508,对该命令进行解析。在一些实施例中,可调用可信计算模块(例如,可信计算模块314)基于解析所述命令来确定货币裁定的债权人、货币裁定的债务人和货币裁定金额。

[0268] 在一些实施例中,可以调用可信计算模块以基于解析所述命令来确定强制执行货币裁定的最后期限,其中,在最后期限之前调用可信计算模块以转账货币裁定金额。

[0269] 在1510,确定账号是否与债权人相关。在一些实施例中,基于可信身份模块,基于身份和记录在区块链上的账户的注册信息来确定账户与债权人相关联。

[0270] 在1512,识别债权人的支付账户和债务人的一个或多个支付账户。在一些实施例中,调用可信计算模块以基于注册信息来识别债权人的支付账户和债务人的一个或多个支付账户,所述债务人的所述一个或多个支付账户的累加余额大于或等于所述货币裁定的金额。

[0271] 在一些实施例中,可信计算模块可以询问债务人的所有支付账户,以识别债务人的一个或多个支付账户,所述债务人的所述一个或多个支付账户的累加余额大于或等于所述货币裁定的金额,而无需询问债务人的所有支付账户的确切余额。所述可信计算模块可以询问该支付账户的余额是否大于一定金额。然后,与支付账户关联的金融机构可以回复“是”或“否”。例如,假设货币裁定是\$20,000,则可信计算模块可以通过询问债务人的每个支付账户是否具有\$20,000的余额来启动。如果一个以上的支付账户回复“是”,则可以随机选择一个支付账户。如果没有支付账户回复“是”,则可信计算模块可以减少询问余额,例如,询问支付账户是否具有\$10,000的余额。可信计算模块可以继续减少询问余额,直到识别出债务人的累加余额大于或等于货币裁定金额的一个或多个支付账户。

[0272] 在1514,转账货币裁定金额。在一些实施例中,可调用可信计算模块以将货币裁定的金额从债务人的一个或多个支付账户转账到债权人的支付账户。在一些实施例中,基于从与一个或多个支付账户相关联的金融机构接收到警报,可以调用可信计算模块以转账货币裁定金额,并且其中所述警报指示从所述一个或多个支付账户中的至少一个支付账户发

起取款请求或转账请求。

[0273] 在一些实施例中,当警报指示与取款请求或转账请求相关联的取款金额或转账金额将使剩余余额小于货币裁定时,可以调用可信计算模块以转账货币裁定金额。例如,假设货币裁定为\$20,000,债务人的支付账户余额为\$30,000,如果取款金额或转账金额为\$20,000,则取款或转账后支付账户的剩余余额为\$10,000,少于货币裁定。然后可以触发警报以指示与取款请求或转账请求相关联的取款金额或转账金额将使剩余余额小于所述货币裁定,并且可以调用可信计算模块来转账货币裁定金额。

[0274] 在一些实施例中,发起取款请求或转账请求的时间与金融机构执行取款请求或转账请求的时间之间存在等待时间,例如24小时。在发起取款请求或转账请求时,可以将来自金融机构的警报发送到可信计算模块。然后,可信计算模块可以确定是否在等待期内转账货币裁定金额。

[0275] 在1516,记录表示转账货币裁定金额的时间的第二经验证时间戳。在一些实施例中,第二经验证时间戳可以由可信时间模块记录。

[0276] 尽管本发明由所附的权利要求书限定,但是应当理解,本发明也可以根据以下实施例来限定:

[0277] 实施例1:一种系统,包括:包括至少一个基于区块链的应用程序的应用层,该应用程序被配置为执行多个步骤以提供服务;以及包括可信时间模块、可信身份模块和可信计算模块的可信服务层;其中,对于所述多个步骤中的至少一些步骤中的每个步骤,所述应用程序被配置为基于使用可信计算模块对区块链数据的处理,执行以下至少一项:从所述可信时间模块获得经验证时间戳、从所述可信身份模块获得经验证身份、或获得计算结果,所述可信计算模块被配置为在区块链中记录关于由应用程序执行的相应步骤的信息,以及经验证时间戳、经验证身份、或计算结果中的至少一个。

[0278] 实施例2:如实施例1所述的系统,其中,可信计算模块被配置为:响应于对与所述服务相关联的经验证记录的请求,提供由所述应用程序执行的多个步骤的经验证记录和与所述多个步骤中的每个步骤相关联的经验证时间戳、经验证身份或计算结果中的至少一个。

[0279] 实施例3:如实施例1或2所述的系统,其中,可信计算模块包括具有TEE的一个或多个数据处理器,所述TEE与一个或多个数据处理器操作系统隔离并且被配置为为一个或多个数据处理器中执行的代码和加载的数据提供增强的机密性和完整性。

[0280] 实施例4:如实施例3所述的系统,其中,基于区块链的应用程序包括可信组件,被配置为:在可信执行环境中执行并记录由该应用程序执行的多个步骤和与所述多个步骤中的每个步骤相关联的经验证时间戳、经验证身份或计算结果中的至少一个。

[0281] 实施例5:如实施例4所述的系统,其中,可信组件包括被配置为基于哈希算法生成表示由该应用程序执行的步骤的数据的哈希值的哈希计算组件。

[0282] 实施例6:如实施例1至5中的任一项所述的系统,其中,基于区块链的应用程序被配置为通过与可信时间模块、可信身份模块或可信计算模块相关联的相应的应用编程接口(API)调用可信时间模块、可信身份模块或可信计算模块的功能。

[0283] 实施例7:如实施例1至6中的任一项所述的系统,其中,可信时间模块被配置为基于(i)国家标准时间信息和/或(ii)从全球定位系统获得的时间信息来生成时间戳。

[0284] 实施例8:如实施例1至7中的任一项所述的系统,其中,可信时间模块被配置为使用与第一用户相关联的第一法院系统承认的第一标准时间来生成与第一用户相关联的时间戳,以及使用与第二用户相关联的第二法院系统承认的第二标准时间来生成与第二用户相关联的时间戳,其中,第一用户和第二用户居住在具有不同法院系统的不同区域中。

[0285] 实施例9:如实施例1至8中的任一项所述的系统,其中,可信身份模块被配置为基于与用户相关联的一个或多个标识验证用户的身份,所述标识包括以下中的至少一个:(i) 移动电话号码、(ii) 信用卡号、(iii) 与在线支付系统关联的用户ID、(iv) 与在线购物账户关联的用户ID、(v) 与音乐流或下载账户相关联的用户ID、(vi) 与电影流或下载账户相关联的用户ID、(vii) 与消息传送或聊天账户相关联的用户ID、(viii) 与在线银行账户相关联的用户ID、(ix) 与约车服务相关联的用户ID、(x) 与在线食品订购服务相关联的用户ID、(xi) 社会保险号、(xii) 驾驶执照号、(xiii) 护照号、(xiv) 与在线游戏服务相关联的用户ID、(xv) 政府实体发布的ID、(xvi) 一个或多个指纹、(xvii) 一个或多个声纹、或(xviii) 虹膜信息。

[0286] 实施例10:如实施例1至9中的任一项所述的系统,其中,可信身份模块被配置为使用与第一用户相关联的第一法院系统承认的第一组标识中的至少一个来验证第一用户的身份,以及使用与第二用户相关联的第二法院系统承认的第二组标识中的至少一个来验证第二用户的身份,其中,第一用户和第二用户居住在具有不同法院系统的不同区域中。

[0287] 实施例11:如实施例1至10中的任一项所述的系统,其中,可信计算模块被配置为根据隐私法律记录与用户相关联的信息。

[0288] 实施例12:如实施例1至11中的任一项所述的系统,其中,基于区块链的应用程序提供使用户能够搜索与卖方提供的产品有关的信息以及为该产品下订单的购物服务,其中,该应用程序被配置为调用可信身份模块以验证用户身份和卖方身份,并调用可信时间模块以验证用户下订单的时间。

[0289] 实施例13:如实施例12所述的系统,其中,基于区块链的应用程序被配置为调用可信计算模块以更新区块链,并且所述区块链被配置为包括表示用户的与为产品下订单相关联的在线活动的的数据。

[0290] 实施例14:如实施例13所述的系统,其中,基于区块链的应用程序被配置为调用可信计算模块以更新所述区块链,从而包括表示在用户发起结账处理后向所述用户显示的信息以及用户向卖方提供的每条信息、用户的身份、卖方的身份以及下订单的时间的数据。

[0291] 实施例15:如实施例14所述的系统,其中,在用户发起结账处理之后向所述用户显示的信息包括对所订购的产品的描述、所述产品的价格、卖方的标识、接收产品的实体的名称、送货地址以及要求用户确认下订单的消息。

[0292] 实施例16:如实施例1至15中的任一项所述的系统,其中,基于区块链的应用程序包括被配置为使用户能够查看网络上的网页并将一个或多个网页的内容保存在存储设备中的网络浏览器,其中,所述应用程序被配置为调用可信身份模块以验证用户的身份,并调用可信时间模块以验证用户查看和/或保存网页的时间。

[0293] 实施例17:如实施例16所述的系统,其中,基于区块链的应用程序被配置为调用可信计算模块以更新所述区块链,并且所述区块链被配置为包括表示由用户查看和/或保存的网页的内容、网页的URL、用户的身份以及显示用户何时查看和/或保存网页的时间戳的

数据。

[0294] 实施例18:如实施例1至17中的任一项所述的系统,其中,基于区块链的应用程序提供使两方或更多方能够在线达成协议的在线协议签署服务,其中,所述应用程序被配置为调用可信身份模块以验证协议各方的身份,以及调用可信时间模块以验证各方签署协议的时间。

[0295] 实施例19:如实施例18所述的系统,其中,基于区块链的应用程序调用可信计算模块以更新所述区块链,所述区块链被配置为包括表示与签署协议相关联的各方的在线活动的的数据。

[0296] 实施例20:如实施例18所述的系统,其中,基于区块链的应用程序调用可信计算模块以更新区块链从而包括表示以下的数据:(i)各方签署的协议的内容、(ii)各方对所述协议进行的修改(如果有的话)(iii)签署协议的各方的身份、以及(iv)显示各方何时签署协议的时间戳。

[0297] 实施例21:一种方法,包括:在基于区块链的可信平台,以多个步骤向用户提供服务;对于所述多个步骤中的每个步骤,执行以下至少一项:从所述可信平台的可信时间模块获得经验证时间戳;从所述可信平台的可信身份模块获得经验证身份,或从所述可信平台的可信计算模块获得计算结果;以及记录与提供给所述用户的所述服务相关联的数据和与区块链中的所述步骤相关联的所述经验证时间戳、所述经验证身份或所述计算结果中的至少一项。

[0298] 实施例22:如实施例21所述的方法,包括:响应于对与所述服务相关联的经验证记录请求,提供由应用程序执行的多个步骤的经验证记录和与所述多个步骤中的每个步骤相关联的经验证时间戳、经验证身份或计算结果中的至少一个。

[0299] 实施例23:如实施例21或22所述的方法,包括:利用可信计算模块使用具有TEE的一个或多个数据处理器以处理区块链的区块链数据,所述TEE与一个或多个数据处理器的操作系统隔离并且被配置为为一个或多个数据处理器中执行的代码和加载的数据提供增强的机密性和完整性。

[0300] 实施例24:如实施例23所述的方法,包括:在可信执行环境中执行与提供服务相关联的可信组件,以及记录提供给用户的服务的多个步骤和与区块链中的所述多个步骤中的每个步骤相关联的经验证时间戳、经验证身份或计算结果中的至少一个。

[0301] 实施例25:如实施例24所述的方法,其中,执行所述可信组件包括基于哈希算法来计算与提供给用户的服务的步骤相关联的数据的哈希值。

[0302] 实施例26:如实施例21至25中的任一项所述的方法,包括:可信平台的基于区块链的应用程序被配置为通过与可信时间模块、可信身份模块或可信计算模块相关联的相应的应用编程接口(API)调用可信时间模块、可信身份模块或可信计算模块的功能。

[0303] 实施例27:如实施例21至26中的任一项所述的方法,包括:在可信时间模块处基于(i)国家标准时间信息和/或(ii)从全球定位系统获得的时间信息来生成时间戳。

[0304] 实施例28:如实施例21至27中的任一项所述的方法,包括:在可信时间模块处使用与第一用户相关联的第一法院系统承认的第一标准时间来生成与第一用户相关联的时间戳,以及使用与第二用户相关联的第二法院系统承认的第二标准时间来生成与第二用户相关联的时间戳,其中,所述第一用户和所述第二用户居住在具有不同法院系统的不同区域

中。

[0305] 实施例29:如实施例21至28中的任一项所述的方法,包括:在可信身份模块处基于与用户相关联的一个或多个标识验证用户的身份,所述标识包括以下中的至少一个:(i) 移动电话号码、(ii) 信用卡号、(iii) 与在线支付系统关联的用户ID、(iv) 与在线购物账户关联的用户ID、(v) 与音乐流或下载账户相关联的用户ID、(vi) 与电影流或下载账户相关联的用户ID、(vii) 与消息传送或聊天账户相关联的用户ID、(viii) 与在线银行账户相关联的用户ID、(ix) 与约车服务相关联的用户ID、(x) 与在线食品订购服务相关联的用户ID、(xi) 社会保险号、(xii) 驾驶执照号、(xiii) 护照号、(xiv) 与在线游戏服务相关联的用户ID、(xv) 政府实体发布的ID、(xvi) 一个或多个指纹、(xvii) 一个或多个声纹、或(xviii) 虹膜信息。

[0306] 实施例30:如实施例21至29中的任一项所述的方法,包括:在可信身份模块处,使用与第一用户相关联的第一法院系统承认的第一组标识中的至少一个来验证第一用户的身份,以及使用与第二用户相关联的第二法院系统承认的第二组标识中的至少一个来验证第二用户的身份,其中,所述第一用户和所述第二用户居住在具有不同法院系统的不同区域中。

[0307] 实施例31:如实施例21至30中的任一项所述的方法,包括:在可信计算模块处根据隐私法律记录与用户相关联的信息。

[0308] 实施例32:如实施例21至31中的任一项所述的方法,其中,提供服务包括:提供使用户能够搜索与卖方提供的产品有关的信息以及为该产品下订单的购物服务,其中,所述方法包括调用可信身份模块以验证用户身份和卖方身份,以及调用可信时间模块以验证用户下订单的时间。

[0309] 实施例33:如实施例32所述的方法,包括:调用可信计算模块以更新区块链,所述区块链被配置为包括表示用户的与为产品下订单相关联的在线活动的的数据。

[0310] 实施例34:如实施例33所述的方法,包括:调用可信计算模块以更新区块链,从而包括表示在用户发起结账处理后向用户显示的信息以及用户向卖方提供的每条信息、用户的身份、卖方的身份以及下订单的时间的数据。

[0311] 实施例35:如实施例34所述的方法,其中,在用户发起结账处理之后向所述用户显示的信息包括对所订购的产品的描述、所述产品的价格、卖方的标识、接收所述产品的实体的名称、送货地址以及要求用户确认下订单的消息。

[0312] 实施例36:如实施例21至35中的任一项所述的方法,其中,提供服务包括:提供被配置为使用户能够查看网络上的网页、并将一个或多个网页的内容保存在存储设备中的网络浏览器,所述方法包括调用可信身份模块以验证用户的身份,以及调用可信时间模块以验证用户查看和/或保存网页的时间。

[0313] 实施例37:如实施例36所述的方法,包括:调用可信计算模块以更新区块链,所述区块链被配置为包括表示由用户查看和/或保存的网页的内容、网页的URL、用户的身份以及显示用户何时查看和/或保存网页的时间戳的数据。

[0314] 实施例38:如实施例21至37中的任一项所述的方法,其中,提供服务包括:提供使两方或更多方能够在线达成协议的在线协议签署服务,所述方法包括调用可信身份模块以验证协议各方的身份,以及调用可信时间模块以验证各方签署协议的时间。

[0315] 实施例39:如实施例38所述的方法,其中,基于区块链的应用程序调用可信计算模

块以更新所述区块链,所述区块链被配置为包括表示与签署协议相关联的各方的在线活动的的数据。

[0316] 实施例40:如实施例38或39所述的方法,包括:调用可信计算模块以更新区块链从而包括表示以下的数据:(i)各方签署的协议的内容、(ii)各方对所述协议进行的修改(如果有的话)、(iii)签署协议的各方的身份、以及(iv)显示各方何时签署协议的时间戳。

[0317] 图16是示出可根据本文实施例执行的处理1600的示例的流程图。处理1600可以由一个或多个区块链节点或通信地耦接到一个或多个区块链节点的计算设备来执行。为了清楚地呈现,以下描述结合本文中的其他附图总体地描述了处理1600。然而,应当理解,处理1600可以例如通过任何系统、环境、软件和硬件,或者系统、环境、软件和硬件的组合来适当地执行。在一些实施例中,处理1600的各个步骤可以并行、组合、循环或以任何顺序运行。

[0318] 在1602,在基于区块链的可信平台上,以多个步骤向用户提供服务。在一些实施例中,所述服务包括向另一用户送达通知。在一些实施例中,所述服务包括向具有争议的两个或更多个用户提供潜在争议解决方案。在一些实施例中,所述服务包括提供法律文档。在一些实施例中,所述服务包括执行法院判决。

[0319] 在1604,对于多个步骤的每个步骤,执行以下至少一项:从可信平台的可信时间模块获得经验证时间戳、从可信平台的可信身份模块获得经验证身份、或从可信平台的可信计算模块获得计算结果。

[0320] 在一些实施例中,可信计算模块用于使用具有TEE的一个或多个数据处理器来处理区块链的区块链数据,该TEE与一个或多个数据处理器的操作系统隔离并且被配置为一个或多个数据处理器中执行的代码和加载的数据提供增强的机密性和完整性。在一些实施例中,在可信执行环境中执行与提供服务相关联的可信组件,并在区块链中记录提供给用户的服务的多个步骤和与所述多个步骤中的每个步骤相关联的经验证时间戳、经验证身份或计算结果中的至少一个。在一些实施例中,执行所述可信组件包括基于哈希算法来计算与提供给所述用户的服务的步骤相关联的数据的哈希值。

[0321] 在一些实施例中,可信平台的基于区块链的应用程序被配置为向用户提供服务,通过与可信时间模块、可信身份模块或可信计算模块相关联的对应的API调用可信时间模块、可信身份模块或可信计算模块的功能。

[0322] 在一些实施例中,可信时间模块基于(i)国家标准时间信息和/或(ii)从全球定位系统获得的时间信息生成时间戳。在一些实施例中,可信时间模块使用与第一用户相关联的第一法院系统承认的第一标准时间来生成与第一用户相关联的时间戳,以及使用与第二用户相关联的第二法院系统承认的第二标准时间来生成与第二用户相关联的时间戳,其中,第一用户和第二用户居住在具有不同法院系统的不同区域中。

[0323] 在一些实施例中,可信身份模块基于与用户相关联的一个或多个标识验证用户的身份,所述标识包括以下中的至少一个:(i)手机号码、(ii)信用卡号、(iii)与在线支付系统关联的用户ID、(iv)与在线购物账户关联的用户ID、(v)与音乐流或下载账户相关联的用户ID、(vi)与电影流或下载账户相关联的用户ID、(vii)与消息传送或聊天账户相关联的用户ID、(viii)与在线银行账户相关联的用户ID、(ix)与约车服务相关联的用户ID、(x)与在线食品订购服务相关联的用户ID、(xi)社会保险号、(xii)驾驶执照号、(xiii)护照号、(xiv)与在线游戏服务相关联的用户ID、(xv)政府实体发布的ID、(xvi)一个或多个指纹、

(xvii) 一个或多个声纹、或(xviii)虹膜信息。在一些实施例中,可信身份模块使用与第一用户相关联的第一法院系统承认的第一组标识中的至少一个来验证第一用户的身份,以及使用与第二用户相关联的第二法院系统承认的第二组标识中的至少一个来验证第二用户的身份,其中,所述第一用户和所述第二用户居住在具有不同法院系统的不同区域中。

[0324] 在一些实施例中,可信计算模块根据隐私法律记录与用户相关联的信息。

[0325] 在1606,将与提供给用户的服务相关联的数据以及与所述步骤相关联的经验证时间戳、经验证身份或计算结果中的至少一个记录在区块链中。

[0326] 可选地,所述处理1600包括:响应于对与所述服务相关联的经验证记录的请求,提供由应用程序执行的多个步骤的经验证记录和与所述多个步骤中的每个步骤相关联的经验证时间戳、经验证身份或计算结果中的至少一个。

[0327] 在一些实施例中,提供服务包括:提供使用户能够搜索与卖方提供的产品有关的信息以及为该产品下订单的购物服务,调用可信身份模块以验证用户身份和卖方身份,以及调用可信时间模块以验证用户下订单的时间。在一些实施例中,调用可信计算模块以更新区块链,所述区块链被配置为包括表示用户的与为产品下订单相关联的在线活动的的数据。在一些实施例中,调用可信计算模块以更新区块链,从而包括表示在用户发起结账处理后向用户显示的信息以及用户向卖方提供的每条信息、用户的身份、卖方的身份以及下订单的时间的数据。在一些实施例中,在用户发起结账处理之后向所述用户显示的信息包括对所订购的产品的描述、所述产品的价格、卖方的标识、接收所述产品的实体的名称、送货地址以及要求用户确认下订单的消息。

[0328] 在一些实施例中,提供服务包括:提供被配置为使用户能够查看网络上的网页、并将一个或多个网页的内容保存在存储设备中的网络浏览器,调用可信身份模块以验证用户的身份,以及调用可信时间模块以验证用户查看和/或保存网页的时间。在一些实施例中,调用可信计算模块以更新区块链,所述区块链被配置为包括表示由用户查看和/或保存的网页的内容、网页的URL、用户的身份以及显示用户何时查看和/或保存网页的时间戳的数据。

[0329] 在一些实施例中,提供服务包括:提供使两方或更多方能够在线达成协议的在线协议签署服务,调用可信身份模块以验证协议各方的身份,以及调用可信时间模块以验证各方签署协议的时间。在一些实施例中,基于区块链的应用程序调用可信计算模块以更新区块链,所述区块链被配置为包括表示与签署协议相关联的各方的在线活动的的数据。在一些实施例中,调用可信计算模块以更新区块链从而包括表示以下的数据:(i)各方签署的协议的内容、(ii)各方对所述协议进行的修改(如果有的话)、(iii)签署协议的各方的身份、以及(iv)显示各方何时签署协议的时间戳。

[0330] 图17是根据本文实施例的装置1700的模块的示例的图。装置1700可以是被配置为向用户提供法律服务的基于区块链的可信平台的实施例的示例。装置1700可以对应于上述实施例,并且装置1700包括以下:提供模块1702,以多个步骤向用户提供服务;可信时间模块1704,提供经验证时间戳;可信身份模块1706,提供经验证身份;可信计算模块1708,提供可信计算结果;和记录模块1710,记录与提供给用户的服务相关联的数据以及与区块链中的步骤相关联的经验证时间戳、经验证身份或计算结果中的至少一个。

[0331] 在可选实施例中,提供模块1702包括基于区块链的可信平台,例如基于区块链的

可信在线平台。

[0332] 在可选实施例中,装置1700还包括提供模块,响应于对与所述服务相关联的经验证记录的请求,提供由应用程序执行的多个步骤的经验证记录和与所述多个步骤中的每个步骤相关联的经验证时间戳、经验证身份或计算结果中的至少一个。

[0333] 在可选实施例中,可信计算模块1708使用具有TEE的一个或多个数据处理器处理区块链的区块链数据,该TEE与一个或多个数据处理器操作系统隔离并且被配置为一个或多个数据处理器中执行的代码以及加载的数据提供增强的机密性和完整性。

[0334] 在可选实施例中,可信计算模块1708在可信执行环境中执行与提供服务相关联的可信组件,以及记录提供给用户的服务的多个步骤和与区块链中的所述多个步骤中的每个步骤相关联的经验证时间戳、经验证身份或计算结果中的至少一个。

[0335] 在可选实施例中,可信组件基于哈希算法来计算与提供给用户的服务的步骤相关联的数据的哈希值。

[0336] 在可选实施例中,基于区块链的可信平台包括向用户提供服务的基于区块链的应用程序,该应用程序通过与可信时间模块1704、可信身份模块1706或可信计算模块1708相关联的对应的应用编程接口(API)调用可信时间模块、可信身份模块或可信计算模块的功能。

[0337] 在可选实施例中,可信时间模块1704基于(i)国家标准时间信息和/或(ii)从全球定位系统获得的时间信息生成时间戳。

[0338] 在可选实施例中,可信时间模块1704使用与第一用户相关联的第一法院系统承认的第一标准时间来生成与第一用户相关联的时间戳,以及使用与第二用户相关联的第二法院系统承认的第二标准时间来生成与第二用户相关联的时间戳,其中,第一用户和第二用户居住在具有不同法院系统的不同区域中。

[0339] 在可选实施例中,可信身份模块1706基于与用户相关联的一个或多个标识验证用户的身份,所述标识包括以下中的至少一个:(i)手机号码、(ii)信用卡号、(iii)与在线支付系统关联的用户ID、(iv)与在线购物账户关联的用户ID、(v)与音乐流或下载账户相关联的用户ID、(vi)与电影流或下载账户相关联的用户ID、(vii)与消息传送或聊天账户相关联的用户ID、(viii)与在线银行账户相关联的用户ID、(ix)与约车服务相关联的用户ID、(x)与在线食品订购服务相关联的用户ID、(xi)社会保险号、(xii)驾驶执照号、(xiii)护照号、(xiv)与在线游戏服务相关联的用户ID、(xv)政府实体发布的ID、(xvi)一个或多个指纹、(xvii)一个或多个声纹、或(xviii)虹膜信息。

[0340] 在可选实施例中,可信身份模块1706使用与第一用户相关联的第一法院系统承认的第一组标识中的至少一个来验证第一用户的身份,以及使用与第二用户相关联的第二法院系统承认的第二组标识中的至少一个来验证第二用户的身份,其中,所述第一用户和所述第二用户居住在具有不同法院系统的不同区域中。

[0341] 在可选实施例中,可信计算模块1708根据隐私法律记录与用户相关联的信息。

[0342] 在可选实施例中,提供模块1702提供使用户能够搜索与卖方提供的产品有关的信息以及为该产品下订单的购物服务,调用可信身份模块1706以验证用户的身份和卖方的身份,以及调用可信时间模块以验证用户下订单的时间。

[0343] 在可选实施例中,调用可信计算模块1708以更新区块链,其中所述区块链被配置

为包括表示用户的与为产品下订单相关联的在线活动的的数据。

[0344] 在可选实施例中,调用可信计算模块1708以更新区块链,从而包括表示在用户发起结账处理后向用户显示的信息以及用户向卖方提供的每条信息、用户的身份、卖方的身份以及下订单的时间的数据。

[0345] 在可选实施例中,在用户发起结账处理之后向所述用户显示的信息包括对所订购的产品的描述、所述产品的价格、卖方的标识、接收所述产品的实体的名称、送货地址以及要求用户确认下订单的消息。

[0346] 在可选实施例中,提供模块1702提供被配置为使用户能够查看网络上的网页、并将一个或多个网页的内容保存在存储设备中的网络浏览器,调用可信身份模块1706以验证用户的身份,以及调用可信时间模块1704以验证用户查看和/或保存网页的时间。

[0347] 在可选实施例中,调用可信计算模块1708以更新区块链,其中所述区块链被配置为包括表示由用户查看和/或保存的网页的内容、网页的URL、用户的身份以及显示用户何时查看和/或保存网页的时间戳的数据。

[0348] 在可选实施例中,提供模块1702提供使两方或更多方能够在线达成协议的在线协议签署服务,调用可信身份模块1706以验证协议各方的身份,以及调用可信时间模块1704以验证各方签署协议的时间。

[0349] 在可选实施例中,基于区块链的应用程序调用可信计算模块以更新区块链,所述区块链被配置为包括表示与签署协议相关联的各方的在线活动的的数据。

[0350] 在可选实施例中,调用可信计算模块1708以更新区块链从而包括表示以下的数据:(i)各方签署的协议的内容、(ii)各方对所述协议进行的修改(如果有的话)、(iii)签署协议的各方的身份、以及(iv)显示各方何时签署协议的时间戳。

[0351] 图18是根据本文实施例的另一装置1800的模块的示例的图。装置1800可以是被配置为在区块链网络中实施传票送达的区块链节点的实施例的示例。装置1800可以对应于前述实施例,装置1800包括以下:接收模块1802,接收基于区块链应用生成的请求,该请求用于将与法律诉讼相关联的通知从送达方递送到被送达方,其中,该请求包括与所述送达方相关联的身份和与所述被送达方相关联的身份;第一确定模块1804,基于所述送达方的身份与所述送达方的记录在区块链上的注册信息中包含的身份之间的匹配,确定所述送达方为所述基于区块链应用的注册用户;记录模块1806,将接收到该请求的时间记录在区块链上;第二确定模块1808,基于与所述被送达方相关联的身份,确定所述被送达方是否为所述基于区块链应用的注册用户;识别模块1810,响应于确定所述被送达方为注册用户,基于所述送达方的注册信息和被送达方的注册信息中包含的可用通信方法,识别递送通知的一种方式或多种方式;递送模块1812,基于所述一种或多种方式中的至少一种方式,向被送达方递送该通知。

[0352] 在可选实施例中,装置1800还包括以下:发送子模块,响应于确定被送达方不是基于区块链应用的注册用户,向与送达方相关联的账户发送通知。

[0353] 在可选实施例中,装置1800还包括以下:确定子模块,在向被送达方递送通知后,确定被送达方是否登录在基于区块链应用上注册的账户;发送子模块,响应于确定被送达方已登录在基于区块链应用上注册的账户,向与送达方相关联的账户发送通知,以通知:通知已被递送。

[0354] 在可选实施例中,装置1800还包括以下:发送子模块,响应于确定被送达方未登陆到在基于区块链应用上注册的账户,向与送达方相关联的账户发送通知,以通知:该被送达方离线。

[0355] 在可选实施例中,装置1800还包括以下:添加子模块,在向被送达方递送通知之前,将时间和基于该时间生成的数字签名添加到该通知。

[0356] 在可选实施例中,装置1800还包括以下:接收子模块,从与被送达方相关联的账户接收对用于接受来自送达方的通知的确认;记录子模块,将接收到确认的时间记录在区块链上;递送子模块,基于送达方的注册信息中包含的可用通信方法,向送达方递送确认。

[0357] 在可选实施例中,可用通信方法包括以下至少一种:电子邮件、电话呼叫或即时消息传送。

[0358] 再次参考图18,它可以被解释为示出了区块链传票送达装置的内部功能模块和结构。区块链传票送达装置可以是配置为在区块链网络中实施传票送达的区块链节点的示例。执行主体本质上可以是电子设备,并且该电子设备包括以下:一个或多个处理器;以及被配置为存储一个或多个处理器的可执行指令的一个或多个计算机可读存储器。在一些实施例中,一个或多个计算机可读存储器耦接至一个或多个处理器且其上存储有编程指令,所述编程指令可由所述一个或多个处理器执行以执行如本文中所述的算法、方法、函数、处理、流程和程序。

[0359] 所描述的主题的实施例可以单独或组合地包括一个或多个特征。例如,在第一实施例中,由区块链节点执行的用于促进基于区块链的传票送达的方法,包括:接收基于区块链应用生成的请求,该请求将与法律诉讼相关的通知从送达方递送到被送达方,其中,该请求包括与所述送达方相关联的身份和与所述被送达方相关联的身份;基于所述送达方的身份与所述送达方的记录在区块链上的注册信息中包含的身份之间的匹配,确定所述送达方为所述基于区块链应用的注册用户;将接收到该请求的时间记录在区块链上;基于与所述被送达方相关联的身份,确定所述被送达方是否为所述基于区块链应用的注册用户;响应于确定所述被送达方为注册用户,基于所述送达方的注册信息和被送达方的注册信息中包含的可用通信方法,识别递送所述通知的一种或多种方式;基于所述一种或多种方式中的至少一种,向被送达方递送该通知。

[0360] 前述和其他描述的实施例可以各自可选地包括一个或多个以下特征:

[0361] 第一特征,可与以下特征中的任意一个组合,指定所述方法还包括:响应于确定被送达方不是基于区块链应用的注册用户,向与送达方相关联的账户发送通知。

[0362] 第二特征,可与之前或之后的任一特征组合,指定所述方法还包括:在向被送达方递送通知之后,确定被送达方是否已登录在基于区块链应用上注册的账户,以及响应于确定被送达方登录在基于区块链应用上注册的账户,向与送达方相关联的账户发送通知以通知:通知已递送。

[0363] 第三特征,可与之前或之后的任一特征组合,指定所述方法还包括:响应于确定被送达方未登录在基于区块链应用中注册的账户,向与送达方相关联的账户发送通知以通知:被送达方离线。

[0364] 第四特征,可与之前或之后的任一特征组合,指定所述方法还包括:在向被送达方递送通知之前,将时间和基于该时间生成的数字签名添加到该通知。

[0365] 第五特征,可与之前或之后的任一特征组合,指定所述方法还包括:从与被送达方相关联的账户接收对用于接受来自送达方的通知的确认;将接收到确认的时间记录在区块链上;基于送达方的注册信息中包含的可用通信方法,向送达方递送该确认。

[0366] 第六特征,可与之前或之后的任一特征组合,指定所述可用通信方法包括以下中的至少一个:电子邮件,电话呼叫或即时消息传送。

[0367] 图19是根据本文实施例的另一装置1900的模块的示例的图。装置1900可以是配置为在区块链网络中执行争议解决处理的区块链节点的实施例的示例。装置1900可以对应于上述的实施例,装置1900包括以下:第一接收模块1902,接收用于解决至少第一方和第二方之间的争议的请求,其中,该请求包括与所述第一方关联的第一身份和与所述第二方关联的第二身份;第一确定模块1904,基于所述第一身份与所述第一方的记录在区块链上的注册信息中包含的身份之间的匹配以及所述第二身份与所述第二方的记录在区块链上的注册信息中包含的身份之间的匹配,确定所述第一方和所述第二方是所述基于区块链应用的注册用户;第一记录模块1906,将接收到该请求的时间记录在区块链上;第二接收模块1908,从在所述基于区块链应用上注册的一个或多个争议解决方案提供者接收一个或多个潜在争议解决方案;第三接收模块1910,接收来自所述第一方的第一选择和来自所述第二方的第二选择,其中,所述第一选择包括第一组一个或多个潜在争议解决方案,所述第二选择包括第二组一个或多个潜在争议解决方案;第二记录模块1912,将接收到所述第一选择的时间记录在区块链上和将接收到所述第二选择的时间记录在区块链上;以及第二确定模块1914,确定(i)在所述第一组一个或多个潜在争议解决方案与所述第二组一个或多个潜在争议解决方案之间存在至少一个共同的潜在争议解决方案、和/或(ii)无一潜在争议解决方案是所述第一方和所述第二方均可接受的。

[0368] 在可选实施例中,用于解决争议的请求包括虚拟资产,并且装置1900还包括以下:发送子模块,将虚拟资产发送到一个或多个争议解决方案提供者中提供至少一个共同的争议解决方案的至少一个争议解决方案提供者。

[0369] 在可选实施例中,装置1900还包括以下:第一接收子模块,从第一方接收用以解决争议的第一请求,该第一请求包括第一虚拟资产;第二接收子模块,从第二方接收用以解决争议的第二请求,所述第二请求包括第二虚拟资产;确定子模块,基于第一虚拟资产和第二虚拟资产中价值较高的一个虚拟资产确定虚拟资产。

[0370] 在可选实施例中,装置1900还包括以下:移除子模块,分别从与第一方关联的第一账户和与第二方关联的第二账户中移除虚拟资产;存储子模块,将从所述第一账户和所述第二账户中移除的虚拟资产存储在区块链上。

[0371] 在可选实施例中,装置1900还包括以下:第一确定子模块,确定第一组一个或多个争议解决方案与第二组一个或多个争议解决方案之间不存在共同的争议解决方案;接收子模块,从不同于争议解决方案提供者的法定授权实体接收争议解决方案;第二确定子模块,确定所述争议解决方案是否与所述第一组一个或多个争议解决方案和所述第二组一个或多个争议解决方案中的争议解决方案匹配;第一发送子模块,响应于确定该争议解决方案与第一组一个或多个争议解决方案最接近匹配,将从第二账户中移除的虚拟资产发送给提供第一组一个或多个争议解决方案中的争议解决方案的争议解决方案提供者;或第二发送子模块,响应于确定该争议解决方案与第二组一个或多个争议解决方案最接近匹配,将从

第一账户中移除的虚拟资产发送给提供第二组一个或多个争议解决方案中的争议解决方案的争议解决方案提供者。

[0372] 在可选实施例中,在预定时间窗内分别从第一方接收第一选择和从第二方接收第二选择。

[0373] 再次参考图19,它可以被解释为示出了区块链争议解决装置的内部功能模块和结构。区块链争议解决装置可以是配置为在区块链网络中实施争议解决处理的区块链节点的示例。执行主体本质上可以是电子设备,并且该电子设备包括以下:一个或多个处理器;以及被配置为存储一个或多个处理器的可执行指令的一个或多个计算机可读存储器。在一些实施例中,一个或多个计算机可读存储器耦接至一个或多个处理器且其上存储有编程指令,所述编程指令可由所述一个或多个处理器执行以执行如本文中所述的算法、方法、函数、处理、流程和程序。

[0374] 所描述的主题的实施例可以单独或组合地包括一个或多个特征。例如,在第一实施例中,用于执行基于区块链的争议解决处理的方法包括:在基于区块链应用处,接收用于解决至少第一方和第二方之间的争议的请求,其中,该请求包括与所述第一方关联的第一身份和与所述第二方关联的第二身份;基于所述第一身份与所述第一方的记录在区块链上的注册信息中包含的身份之间的匹配以及所述第二身份与所述第二方的记录在区块链上的注册信息中包含的身份之间的匹配,确定所述第一方和所述第二方是所述基于区块链应用的注册用户;将接收到该请求的时间记录在区块链上;从在所述基于区块链应用中注册的一个或多个争议解决方案提供者接收一个或多个潜在争议解决方案;接收来自所述第一方的第一选择和来自所述第二方的第二选择,其中,所述第一选择包括第一组一个或多个潜在争议解决方案,所述第二选择包括第二组一个或多个潜在争议解决方案;将接收到所述第一选择的时间记录在区块链上和将接收到所述第二选择的时间记录在区块链上;以及确定(i)在所述第一组一个或多个潜在争议解决方案与所述第二组一个或多个潜在争议解决方案之间存在至少一个共同的潜在争议解决方案,和/或(ii)无一潜在争议解决方案是所述第一方和所述第二方均可接受的。

[0375] 前述和其他描述的实施例可以各自可选地包括一个或多个以下特征:

[0376] 第一特征,可与以下任一特征组合,指定用于解决争议的请求包括虚拟资产,以及所述方法包括将虚拟资产发送到一个或多个争议解决方案提供者中提供至少一个共同的争议解决方案的至少一个争议解决方案提供者。

[0377] 第二特征,可与之前或之后的任一特征组合,指定所述方法还包括:从第一方接收用以解决争议的第一请求,该第一请求包括第一虚拟资产;从第二方接收用以解决争议的第二请求,所述第二请求包括第二虚拟资产;以及基于第一虚拟资产和第二虚拟资产中价值较高的一个虚拟资产来确定虚拟资产。

[0378] 第三特征,可与之前或之后的任一特征组合,指定所述方法还包括:分别从与第一方关联的第一账户和与第二方关联的第二账户中移除虚拟资产;以及将从所述第一账户和所述第二账户中移除的虚拟资产存储在区块链上。

[0379] 第四特征,可与之前或之后的任一特征组合,指定所述方法还包括:确定第一组一个或多个争议解决方案与第二组一个或多个争议解决方案之间没有共同的争议解决方案;从不同于争议解决方案提供者的法定授权实体接收争议解决方案;确定所述争议解决方案

是否与所述第一组一个或多个争议解决方案和所述第二组一个或多个争议解决方案中的争议解决方案相匹配;响应于确定该争议解决方案与第一组一个或多个争议解决方案中的争议解决方案最接近匹配,将从第二账户中移除的虚拟资产发送给提供第一组一个或多个争议解决方案中的争议解决方案的争议解决方案提供者;或响应于确定该争议解决方案与第二组一个或多个争议解决方案中的争议解决方案最接近匹配,将从第一账户中移除的虚拟资产发送给提供第二组一个或多个争议解决方案中的争议解决方案的争议解决方案提供者。

[0380] 第五特征,可与之前或之后的任一特征组合,指定在预定时间窗内分别从第一方接收第一选择和从第二方接收第二选择。

[0381] 图20是根据本文实施例的另一装置2000的模块的示例的图。装置2000可以是配置为处理信息的区块链节点的实施例的示例。装置2000可以对应于上述实施例,装置2000包括以下:接收模块2002,接收从与基于区块链应用相关联的用户的账户发起的请求,该请求用于提供服务,其中,该请求包括与该用户相关联的身份;确定模块2004,基于所述身份与记录在区块链上的所述基于区块链应用相关联的用户的注册信息中包含的身份之间的匹配,确定所述用户为所述基于区块链应用的注册用户;识别模块2006,识别用于提供服务的多个步骤中要填写并提交的一个或多个电子表格;生成模块2008,在所述多个步骤中的每个步骤中,基于执行所述步骤的时间和此时所述电子表格上的数字内容生成唯一标识(ID);第一记录模块2010,在所述多个步骤中的每个步骤中,将所述唯一ID、所述时间和所述数字内容记录在区块链上;嵌入模块2012,在所述多个步骤中的每个步骤中,通过更改与所述数字内容相关联的一个或多个属性来表示所述唯一ID,将所述唯一ID嵌入到此时的数字内容中,其中,该嵌入会生成能够基于所述唯一ID从所述区块链检索所述时间和所述数字内容的嵌入信息的数字内容;以及第二记录模块2014,在所述多个步骤中的每个步骤中,将所述嵌入信息的数字内容记录到区块链。

[0382] 在可选实施例中,该请求是第一请求,并且装置2000还包括以下:接收子模块,接收从与基于区块链应用相关联的服务提供者的账户发起的第二请求,其中,第二请求用于处理第一请求,第二请求包括与服务提供者相关联的身份;确定子模块,基于服务提供者关联的身份与服务提供者的记录在区块链上的注册信息中包含的身份之间的匹配,确定服务提供者基于区块链应用的注册服务提供者。

[0383] 在可选实施例中,用户和服务提供者执行多个步骤。

[0384] 在可选实施例中,在用户执行的多个步骤中的每个步骤中,基于时间和此时用户填写在电子表格上的数字内容来生成唯一ID,其中,该唯一ID嵌入到用户填写的数字内容中。

[0385] 在可选实施例中,唯一ID为第一唯一ID,装置2000还包括以下:生成子模块,在服务提供者执行的多个步骤中的每个步骤中,基于执行所述步骤的时间和此时服务提供者填写的电子表格中的数字内容生成第二唯一ID;以及嵌入子模块,在服务提供者执行的多个步骤中的每个步骤中,将所述第二唯一ID嵌入到服务提供者填写的数字内容中。

[0386] 在可选实施例中,电子表格和嵌入信息的数字内容之间的视觉差异对于肉眼不明显可见。

[0387] 在可选实施例中,唯一ID是基于哈希函数和/或非对称加密来生成的。

[0388] 在可选实施例中,嵌入唯一ID是基于使用离散小波变换、离散余弦变换、奇异值分解、最低有效位或不可检测的隐写中的一个或多个的数字水印处理来执行的。

[0389] 在可选实施例中,与数字内容相关联的一个或多个属性包括数字内容的颜色、大小、方向、形状和字体中的一个或多个。

[0390] 在可选实施例中,身份包括以下至少一个:(i) 手机号码、(ii) 信用卡号、(iii) 与在线支付系统关联的用户ID、(iv) 与在线购物账户关联的用户ID、(v) 与音乐流或下载账户相关联的用户ID、(vi) 与电影流或下载账户相关联的用户ID、(vii) 与消息传送或聊天账户相关联的用户ID、(viii) 与在线银行账户相关联的用户ID、(ix) 与约车服务相关联的用户ID、(x) 与在线食品订购服务相关联的用户ID、(xi) 社会保险号、(xii) 驾驶执照号、(xiii) 护照号、(xiv) 与在线游戏服务相关联的用户ID、或(xv) 政府实体发布的ID。

[0391] 再次参考图20,它可以被解释为示出了区块链信息处理装置的内部功能模块和结构。区块链信息处理装置可以是配置为在区块链网络中实施信息处理的区块链节点的示例。执行主体本质上可以是电子设备,并且该电子设备包括以下:一个或多个处理器;以及被配置为存储一个或多个处理器的可执行指令的一个或多个计算机可读存储器。在一些实施例中,一个或多个计算机可读存储器耦接至一个或多个处理器且其上存储有编程指令,所述编程指令可由所述一个或多个处理器执行以执行如本文中所述的算法、方法、函数、处理、流程和程序。

[0392] 所描述的主题的实施例可以单独或组合地包括一个或多个特征。例如,在第一实施例中,区块链节点执行的基于区块链的信息处理方法包括:接收从与基于区块链应用相关联的用户的账户发起的请求,该请求用于提供服务,其中,该请求包括与该用户相关联的身份;基于所述身份与记录在区块链上的所述基于区块链应用相关联的用户的注册信息中包含的身份之间的匹配,确定所述用户为所述基于区块链应用的注册用户;识别用于提供该服务的多个步骤中要填写并提交的一个或多个电子表格;在所述多个步骤中的每个步骤中:基于执行所述步骤的时间和此时所述电子表格上的数字内容生成唯一标识(ID);将所述唯一ID、所述时间和所述数字内容记录在区块链上;在所述多个步骤中的每个步骤中:通过更改与所述数字内容相关联的一个或多个属性来表示所述唯一ID,将所述唯一ID嵌入此时的数字内容中,其中,该嵌入会生成能够基于所述唯一ID从所述区块链检索所述时间和所述数字内容的嵌入信息的数字内容;以及在所述多个步骤中的每个步骤中,将所述嵌入信息的数字内容记录到区块链。

[0393] 前述和其他描述的实施例可以各自可选地包括一个或多个以下特征:

[0394] 第一特征,可与以下任一特征组合,指定所述请求为第一请求,所述方法还包括:接收从与基于区块链应用相关联的服务提供者的账户发起的第二请求,其中,第二请求用于处理第一请求,第二请求包括与服务提供者相关联的身份;以及,基于服务提供者关联的身份与服务提供者的记录在区块链上的注册信息中包含的身份之间的匹配,确定服务提供者基于区块链应用的注册服务提供者。

[0395] 第二特征,可与之前或之后的任一特征组合,指定用户和服务提供者执行多个步骤。

[0396] 第三特征,可与之前或之后的任一特征组合,指定在用户执行的多个步骤中的每个步骤中,基于时间和此时用户填写在电子表格上的数字内容来生成唯一ID,其中,该唯一

ID嵌入到用户填写的数字内容中。

[0397] 第四特征,可与之前或之后的任一特征中组合,指定该唯一ID是第一唯一ID,并且该方法还包括:在服务提供者执行的多个步骤中的每个步骤中:基于执行步骤的时间以及此时服务提供者填写在电子表格上的数字内容生成第二唯一ID;在服务提供者执行的多个步骤中的每个步骤中:将第二唯一ID嵌入服务提供者填写的数字内容中。

[0398] 第五特征,可与之前或之后的任一特征组合,指定电子表格和嵌入信息的内容之间的视觉差异对于肉眼不明显可见。

[0399] 第六特征,可与之前或之后的任一特征组合,指定所述唯一ID是基于哈希函数和/或非对称加密生成的。

[0400] 第七特征,可与之前或之后的任一特征组合,指定所述嵌入唯一ID是基于使用离散小波变换、离散余弦变换、奇异值分解、最低有效位或隐写术中的一个或多个的数字水印处理来执行的。

[0401] 第八特征,可与之前或之后的任一特征组合,指定与所述数字内容相关联的一个或多个属性包括数字内容的颜色、大小、方向、形状和字体中的一个或多个。

[0402] 第九特征,可与之前或之后的任一特征组合,指定所述身份包括以下至少一个:(i) 手机号码、(ii) 信用卡号、(iii) 与在线支付系统关联的用户ID、(iv) 与在线购物账户关联的用户ID、(v) 与音乐流或下载账户相关联的用户ID、(vi) 与电影流或下载账户相关联的用户ID、(vii) 与消息传送或聊天账户相关联的用户ID、(viii) 与在线银行账户相关联的用户ID、(ix) 与约车服务相关联的用户ID、(x) 与在线食品订购服务相关联的用户ID、(xi) 社会保险号、(xii) 驾驶执照号、(xiii) 护照号、(xiv) 与在线游戏服务相关联的用户ID、或(xv) 政府实体发布的ID。

[0403] 图21是根据本文实施例的另一装置2100的模块的示例的图。装置2100可以是配置为处理法院判决的区块链节点的实施例的示例。装置2100可以对应于上述实施例,装置2100包括以下:接收模块2102,接收与基于区块链应用的账户相关联的请求,所述请求用于收集法院命令中发布的货币裁定,其中,所述请求包括与该账户相关联的身份;第一确定模块2104,基于与记录在区块链上的所述命令相关联的哈希值之间的匹配来确定该命令是真实的;第一记录模块2106,将表示接收到所述请求的时间的第一经验证时间戳记录在所述区块链上;第一调用模块2108,调用所述可信计算模块,以基于解析所述命令来确定所述货币裁定的债权人、所述货币裁定的债务人和所述货币裁定的金额;第二确定模块2110,基于所述可信身份模块,基于所述身份和记录在所述区块链上的所述账户的注册信息,确定所述账户与所述债权人相关联;第二调用模块2112,调用所述可信计算模块,以基于所述注册信息,来识别所述债权人的支付账户和所述债务人的一个或多个支付账户,所述债务人的所述一个或多个支付账户的累加余额大于或等于所述货币裁定的金额;第三调用模块2114,调用所述可信计算模块,以将所述货币裁定的金额从所述债务人的一个或多个支付账户转账到所述债权人的支付账户;以及第二记录模块2116,记录表示所述货币裁定的金额被转账的时间的第二经验证时间戳。

[0404] 在可选实施例中,装置2100还包括以下:接收子模块,在接收第一请求之前,接收与基于区块链应用的第二账户相关联的第二请求、该第二请求用于记录法院的命令,其中,第二请求包括与第二账户相关联的身份;确定子模块,基于可信身份模块,基于与第二账户

相关联的身份和记录在区块链上的第二账户的注册信息,确定第二账户与法院相关联;调用子模块,调用可信计算模块以将命令在区块链上记录为命令的哈希值;以及记录子模块,记录表示将命令记录在区块链上的时间的第三经验证时间戳。

[0405] 在可选实施例中,装置2100还包括以下:调用子模块,调用可信计算模块以从一个或多个支付账户中获取等于货币裁定的金额的累加货币金额。

[0406] 在可选实施例中,装置2100还包括以下:调用子模块,调用可信计算模块以基于解析所述命令来确定强制执行货币裁定的最后期限,其中,在最后期限之前调用可信计算模块以转账货币裁定的金额。

[0407] 在可选实施例中,调用可信计算模块,以基于从与一个或多个支付账户相关联的金融机构接收到警报转账货币裁定金额,其中,所述警报指示从所述一个或多个支付账户中的至少一个账户发起取款请求或转账请求。

[0408] 再次参考图21,它可以被解释为示出了区块链执行装置的内部功能模块和结构。区块链执行装置可以是配置为在区块链网络中实施判决执行的区块链节点的示例。执行主体本质上可以是电子设备,并且该电子设备包括以下:一个或多个处理器;以及配置为存储一个或多个处理器的可执行指令的一个或多个计算机可读存储器。在一些实施例中,一个或多个计算机可读存储器耦接至一个或多个处理器且其上存储有编程指令,所述编程指令能够由所述一个或多个处理器执行以执行如本文中所述的算法、方法、函数、处理、流程和程序。

[0409] 所描述的主题的实施例可以单独或组合地包括一个或多个特征。例如,在第一实施例中,由区块链节点执行的用于处理法院判决的方法包括:接收与基于区块链应用的账户相关联的请求,所述请求用于收集法院命令中发布的货币裁定,其中,所述请求包括与该账户相关联的身份;以及由可信身份模块基于与记录在区块链上的所述命令相关联的哈希值之间的匹配来确定该命令是真实的;可信时间模块将表示接收到所述请求的时间的第一经验证时间戳记录在所述区块链上;调用所述可信计算模块,以基于解析所述命令确定所述货币裁定的债权人、所述货币裁定的债务人和所述货币裁定的金额;基于所述可信身份模块,基于所述身份和记录在所述区块链上的所述账户的注册信息,确定所述账户与所述债权人相关联;调用所述可信计算模块,以基于所述注册信息,识别所述债权人的支付账户和所述债务人的一个或多个支付账户,所述债务人的所述一个或多个支付账户的累加余额大于或等于所述货币裁定的金额;调用所述可信计算模块,以将所述货币裁定的金额从所述债务人的所述一个或多个支付账户转账到所述债权人的支付账户;以及所述可信时间模块记录表示所述货币裁定的金额被转账的时间的第二经验证时间戳。

[0410] 前述和其他描述的实施例可以各自可选地包括一个或多个以下特征:

[0411] 第一特征,可与以下任一特征组合,指定所述请求为第一请求,所述账户为第一账户,所述方法还包括:在接收所述第一请求之前,接收与基于区块链应用的第二账户相关联的第二请求、所述第二请求用于记录法院命令,其中,所述第二请求包括与第二账户相关联的身份;基于可信身份模块,基于与第二账户相关联的身份和记录在区块链上的与第二账户的注册信息,确定第二账户与法院相关联;调用可信计算模块以将命令在区块链上记录为命令的哈希值;以及可信时间模块记录表示将命令记录在区块链上的时间的第三经验证时间戳。

[0412] 第二特征,可与之前或之后任一特征组合,指定所述方法还包括:调用可信计算模块以从一个或多个支付账户中获取等于货币裁定的金额的累加货币金额。

[0413] 第三特征,可与之前或之后任一特征组合,指定所述方法还包括:调用可信计算模块以基于解析所述命令确定强制执行货币裁定的最后期限,其中,在最后期限之前调用可信计算模块以转账货币裁定金额。

[0414] 第四特征,可与之前或之后任一特征组合,指定调用可信计算模块以基于从与所述一个或多个支付账户相关联的金融机构接收到警报转账货币裁定的金额,其中,所述警报指示从所述一个或多个支付账户中的至少一个账户发起取款请求或转账请求。

[0415] 前述实施例中示出的系统、装置、模块或单元可以通过使用计算机芯片或实体来实施,或者可以通过使用具有特定功能的产品来实施。典型的实施例设备是计算机,计算机可以是个人计算机、膝上型计算机、蜂窝电话、相机电话、智能移动电话、个人数字助理、媒体播放器、导航设备、电子邮件传送设备、游戏控制台、平板计算机、可穿戴设备或这些设备的任意组合。

[0416] 对于装置中每个模块的功能和作用的实施例处理,可以参考前一方法中相应步骤的实施例处理。为简单起见,这里省略了细节。

[0417] 由于装置实施基本上对应于方法实施,对于相关部件,可以参考方法实施中的相关描述。先前描述的装置实施仅是示例。被描述为单独部分的模块可以或不是物理上分离的,并且显示为模块的部分可以是或不是物理模块,可以位于一个位置,或者可以分布在多个网络模块上。可以基于实际需求来选择一些或所有模块,以实现本文方案的目标。本领域的普通技术人员无需付出创造性劳动就能理解和实现本申请的实施例。

[0418] 本文中描述的主题、动作和操作的实施可以在数字电子电路、有形体现的计算机软件或固件、计算机硬件中实施,包括本文中公开的结构及其结构等同物,或者它们中的一个或多个的组合。本文中描述的主题的实施可以实现为一个或多个计算机程序,例如,编码在计算机程序载体上的一个或多个计算机程序指令模块,用于由数据处理装置执行或控制数据处理装置的操作。例如,计算机程序载体可以包括一个或多个计算机可读存储介质,其上编码或存储有指令。载体可以是有形的非暂态计算机可读介质,诸如磁盘、磁光盘或光盘、固态驱动器、随机存取存储器(RAM)、只读存储器(ROM)或其他类型的介质。可选地或附加地,载体可以是人工生成的传播信号,例如,机器生成的电信号、光信号或电磁信号,其被生成来编码信息用于传输到合适的接收器装置以供数据处理装置执行。计算机存储介质可以是或可以部分是机器可读存储设备、机器可读存储基板、随机或串行访问存储器设备或它们中的一个或多个的组合。计算机存储介质不是传播信号。

[0419] 计算机程序,也可以被称为或描述为程序、软件、软件应用程序、app、模块、软件模块、引擎、脚本或代码,可以以任何形式的编程语言编写,包括编译或解释性语言、或声明或程序性语言;它可以配置为任何形式,包括作为独立程序,或作为模块、组件、引擎、子程序或适合在计算环境中执行的其他单元,该环境可包括由数据通信网络互连的一个或多个位置上的一台或多台计算机。

[0420] 计算机程序可以但非必须对应于文件系统中的文件。计算机程序可以存储在:保存其他程序或数据的文件的一部分中,例如,存储在标记语言文档中的一个或多个脚本;专用于所讨论的程序的单个文件;或者多个协调文件,例如,存储一个或多个模块、子程序或

代码部分的多个文件。

[0421] 用于执行计算机程序的处理器包括：例如，通用和专用微处理器两者，和任意种类的数字计算机的任意一个或多个处理器。通常，处理器将接收用于执行的计算机程序的指令以及来自耦接至处理器的非暂态计算机可读介质的数据。

[0422] 术语“数据处理装置”包括用于处理数据的所有种类的装置、设备和机器，例如包括可编程处理器、计算机或多个处理器或计算机。数据处理装置可以包括例如FPGA（现场可编程门阵列）、ASIC（专用集成电路）或GPU（图形处理单元）的专用逻辑电路。除了硬件，该装置还可以包括为计算机程序创建执行环境的代码，例如，构成处理器固件、协议栈、数据库管理系统、操作系统或者它们中一个或多个的组合的代码。

[0423] 本文中描述的处理和逻辑流程可以由执行一个或多个计算机程序的一台或多台计算机或处理器执行，以通过对输入数据进行操作并生成输出来执行操作。处理和逻辑流程也可以由例如FPGA、ASIC或GPU等的专用逻辑电路或专用逻辑电路与一个或多个编程计算机的组合来执行。

[0424] 适合于执行计算机程序的计算机可以基于通用和/或专用微处理器，或任何其他种类的中央处理单元。通常，中央处理单元将从只读存储器和/或随机存取存储器接收指令和数据。计算机的元件可包括用于执行指令的中央处理单元和用于存储指令和数据的一个或多个存储设备。中央处理单元和存储器可以补充有专用逻辑电路或集成在专用逻辑电路中。

[0425] 通常，计算机还将包括或可操作地耦接至一个或多个存储设备，以从一个或多个存储设备接收数据或向一个或多个存储设备传送数据。大容量存储设备可以是例如，磁盘、磁光盘或光盘、固态驱动器或任何其他类型的非暂态计算机可读介质。但是，计算机不是必须具有这样的设备。因此，计算机可以耦接到例如一个或多个存储器的本地和/或远程的一个或多个大容量存储设备。例如，计算机可以包括作为计算机的组成部件的一个或多个本地存储器，或者计算机可以耦接到云网络中的一个或多个远程存储器。此外，计算机可以嵌入在另一设备中，例如移动电话、个人数字助理（PDA）、移动音频或视频播放器、游戏控制台、全球定位系统（GPS）接收器或例如通用串行总线（USB）闪存驱动器的便携式存储设备，这里仅举几例。

[0426] 组件可以通过直接或经由一个或多个中间件例如电连接或光连接地彼此连接通信而彼此“耦接”。如果部件中的一个部件被集成到另一个中，则部件也可以被彼此“耦接”。例如，集成到处理器中的大容量存储组件（例如，L2高速缓存组件）被“耦接到”处理器。

[0427] 为了提供与用户的交互，本文中描述的主题的实施例可以在计算机上实现或配置为与该计算机通信，该计算机具有：显示设备，例如，LCD（液晶显示器）监视器，用于向用户显示信息；以及输入设备，用户可以通过该输入设备向计算机提供输入，例如键盘和例如鼠标、轨迹球或触摸板等的指针设备。其他类型的设备也可用于提供与用户的交互；例如，提供给用户的反馈可以是任何形式的感官反馈，例如视觉反馈、听觉反馈或触觉反馈；并且可以接收来自用户任何形式的输入，包括声音、语音输入或触觉输入。此外，计算机可以通过向用户使用的设备发送文档和从用户使用的设备接收文档来与用户交互；例如，通过向用户设备上的web浏览器发送web页面以响应从web浏览器收到的请求，或者通过与例如智能电话或电子平板电脑等的用户设备上运行的应用程序（app）进行交互。此外，计算机可以通

过向个人设备(例如,运行消息传送应用程序的智能移动电话)轮流发送文本消息或其他形式的消息来并且从用户接收响应消息来与用户交互。

[0428] 本文使用与系统,装置和计算机程序组件有关的术语“配置为”。对于被配置为执行特定操作或动作的一个或多个计算机的系统,意味着系统已经在其上安装了在运行中促使该系统执行所述操作或动作的软件、固件、硬件或它们的组合。对于被配置为执行特定操作或动作的一个或多个计算机程序,意味着一个或多个程序包括当被数据处理装置执行时促使该装置执行所述操作或动作的指令。对于被配置为执行特定操作或动作的专用逻辑电路,意味着该电路具有执行所述操作或动作的电子逻辑。

[0429] 虽然本文包含许多具体实施细节,但是这些细节不应被解释为由权利要求本身限定的对要求保护的范围的限制,而是作为对特定实施例的具体特征的描述。在本文中单个实施例的上下文中描述的多个特征也可以在单个实施例中组合实现。相反,在单个实施方式上下文中描述的各种特征也可以单独地或以任何合适的子组合在多个实施方式中实现。此外,尽管上面的特征可以描述为以某些组合起作用并且甚至最初如此要求保护,但是在一些情况下可以从要求保护的组合中删除该组合的一个或多个特征,并且可以要求保护指向子组合或子组合的变体。

[0430] 类似地,虽然以特定顺序在附图中描绘了操作并且在权利要求中叙述了操作,但是这不应该被理解为:为了达到期望的结果,要求以所示的特定顺序或依次执行这些操作,或者要求执行所有示出的操作。在某些情况下,多任务和并行处理可能是有利的。此外,上述实施例中的各种系统模块和组件的划分不应被理解为在所有实施例中都要求如此划分,而应当理解,所描述的程序组件和系统通常可以一起集成在单个软件产品中或打包成多个软件产品。

[0431] 已经描述了主题的特定实施方式。其他实施方式在以下权利要求的范围内。例如,权利要求中记载的动作可以以不同的顺序执行并且仍然实现所期望的结果。作为一个示例,附图中描绘的过程无需要求所示的特定顺序或次序来实现期望的结果。在一些情况下,多任务和并行处理可能是有利的。

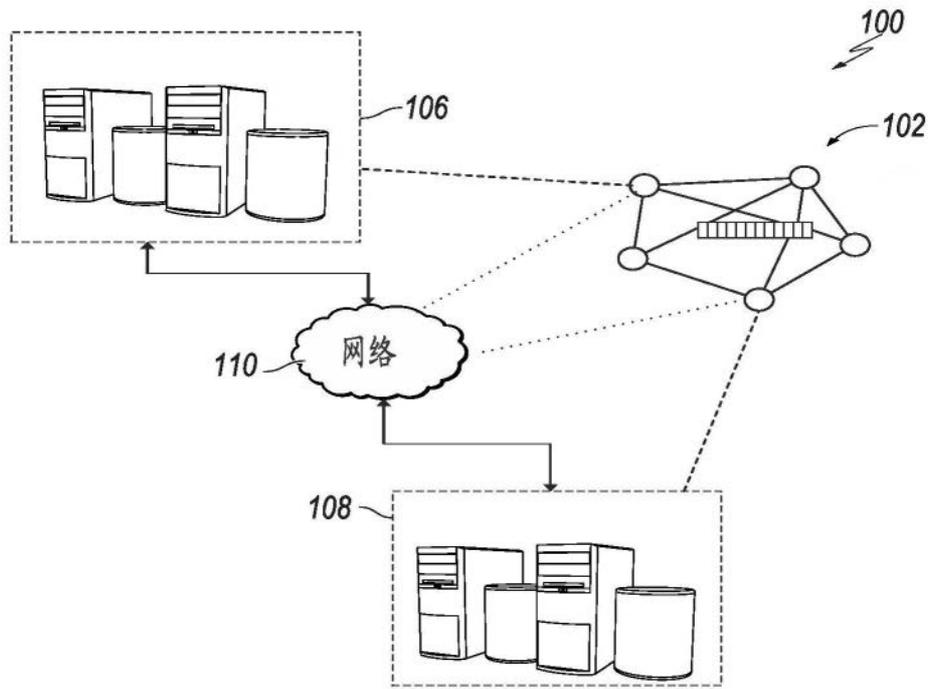


图1

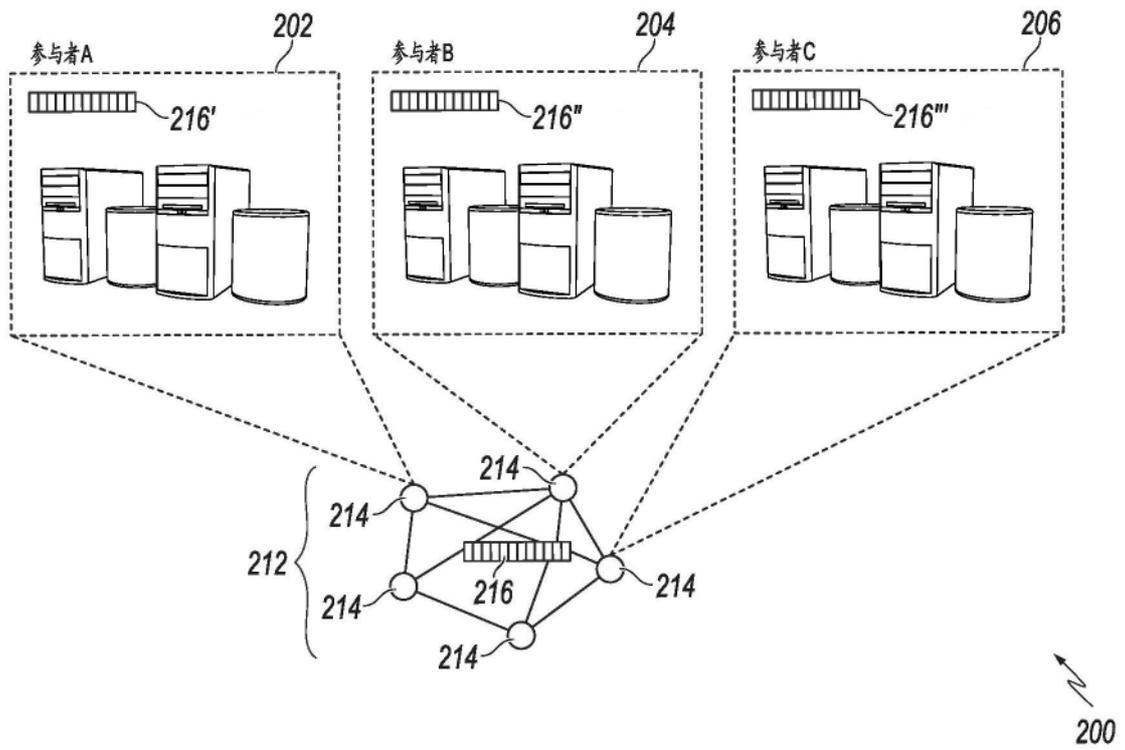


图2

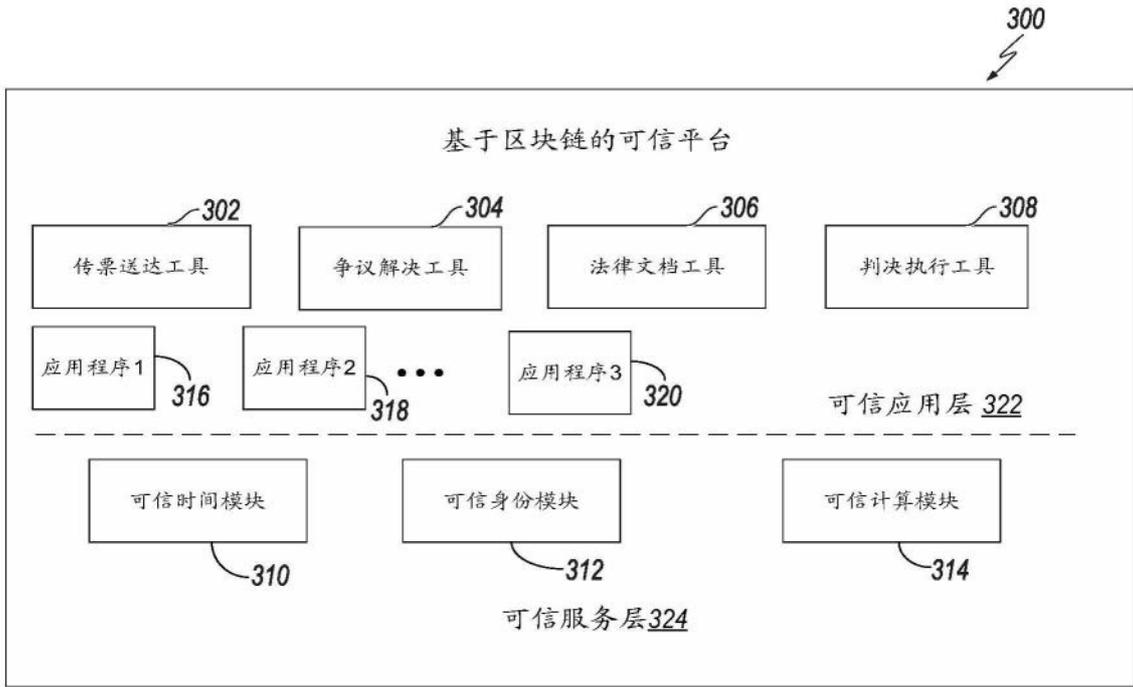


图3

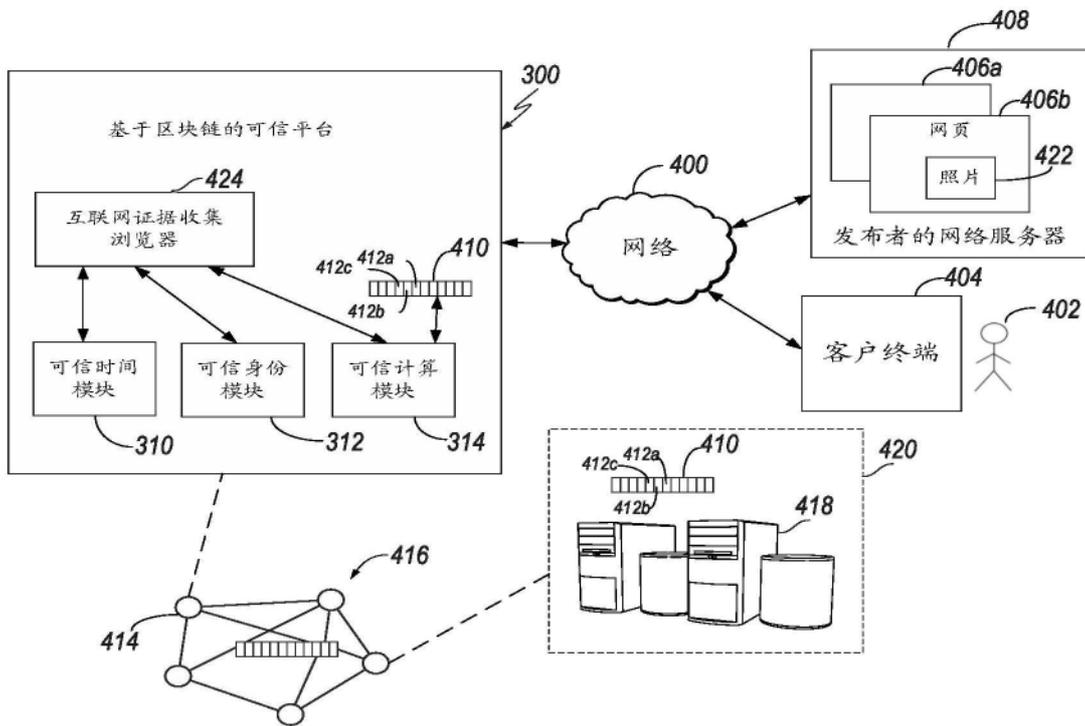


图4

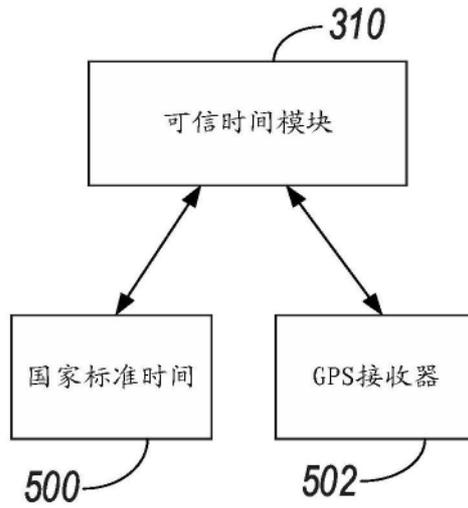


图5

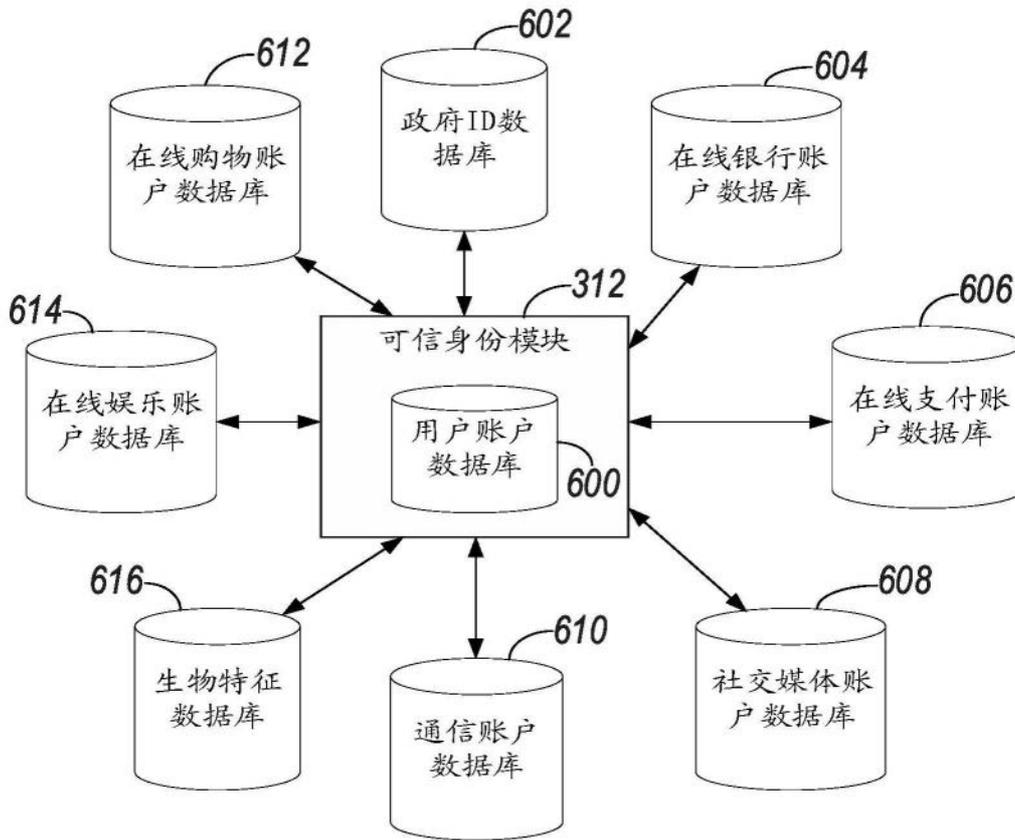


图6

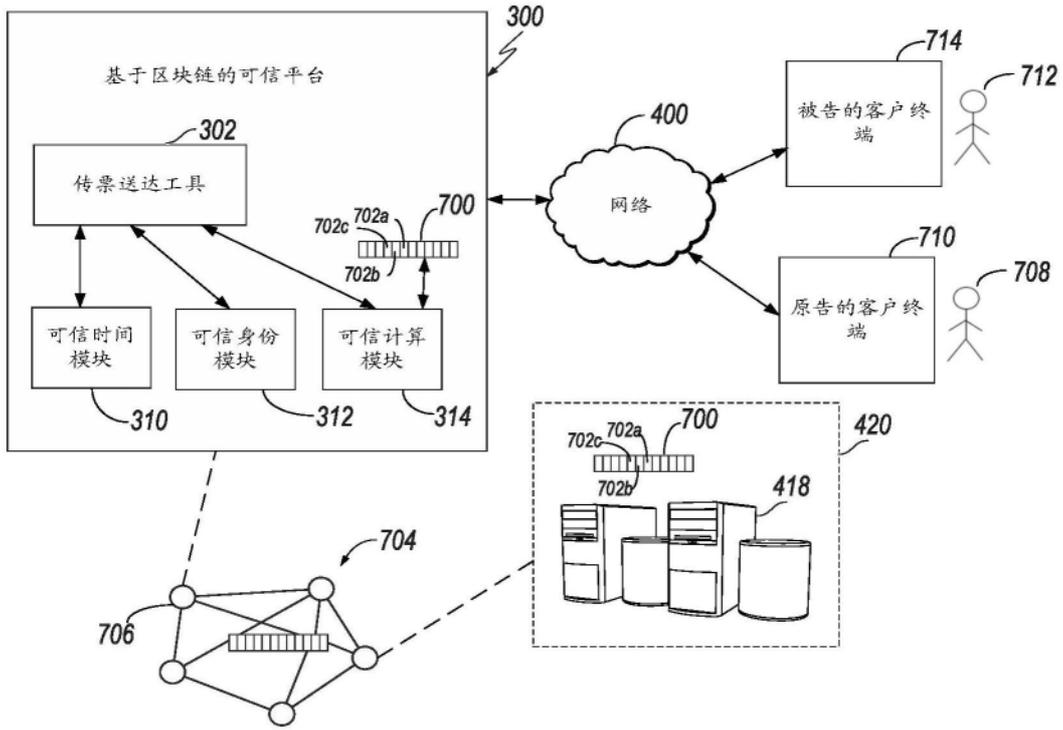


图7

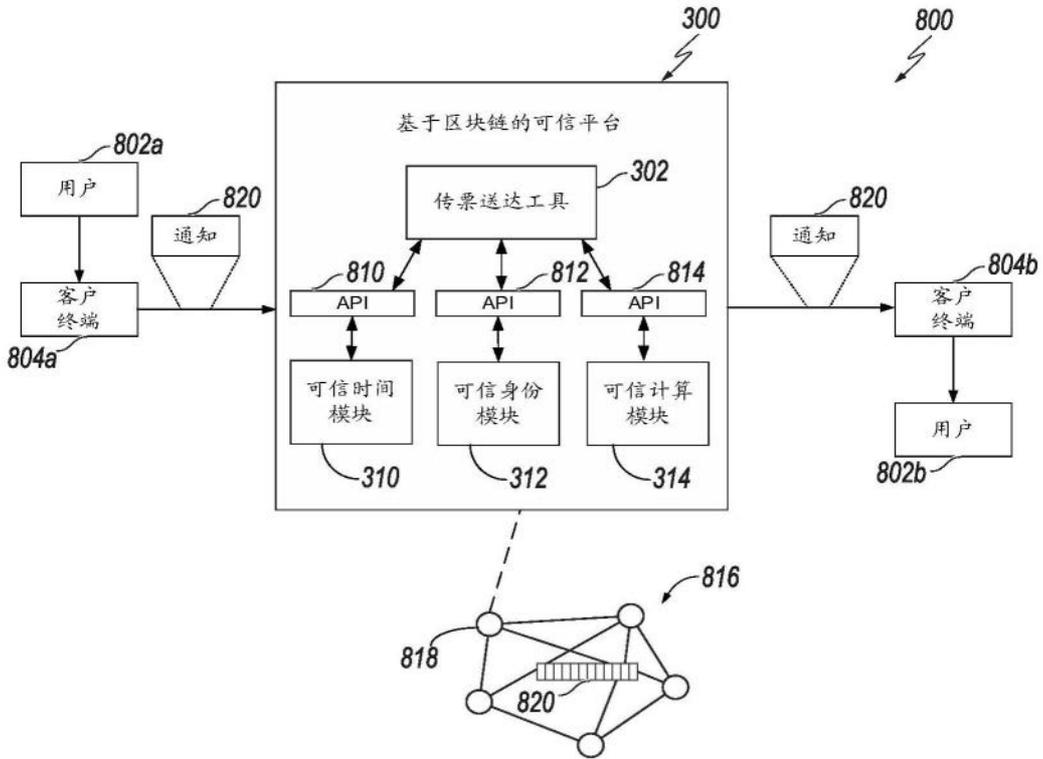


图8

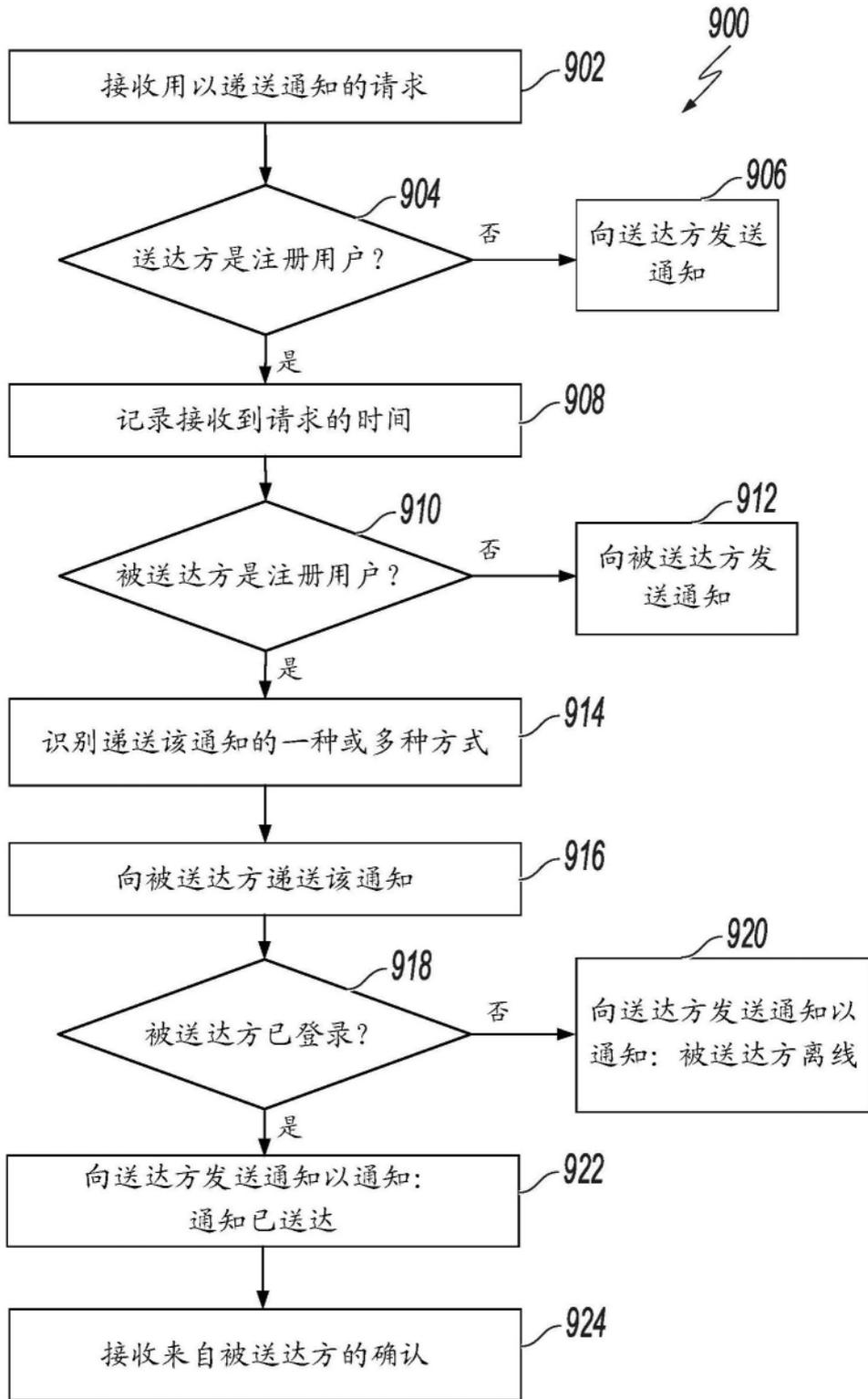


图9

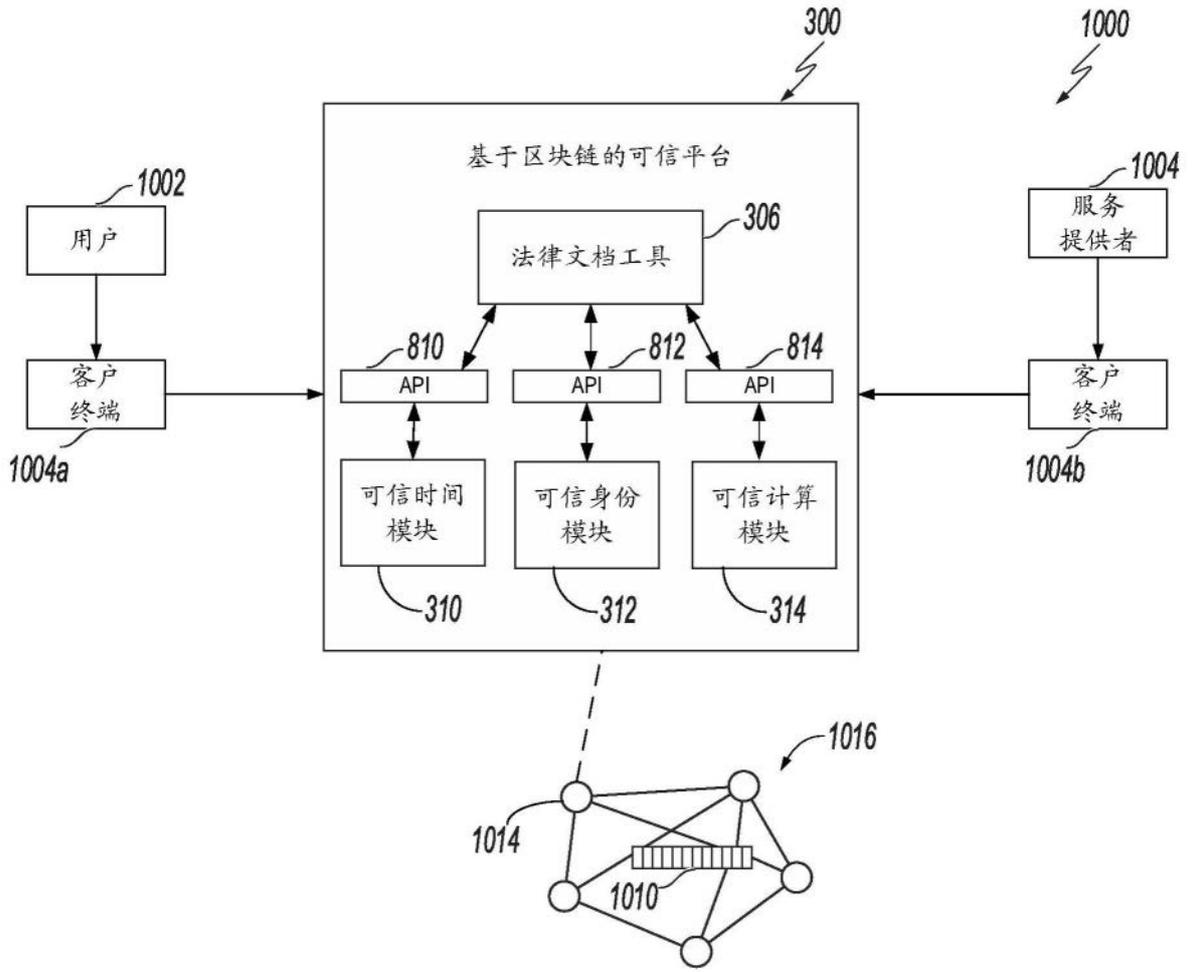


图10

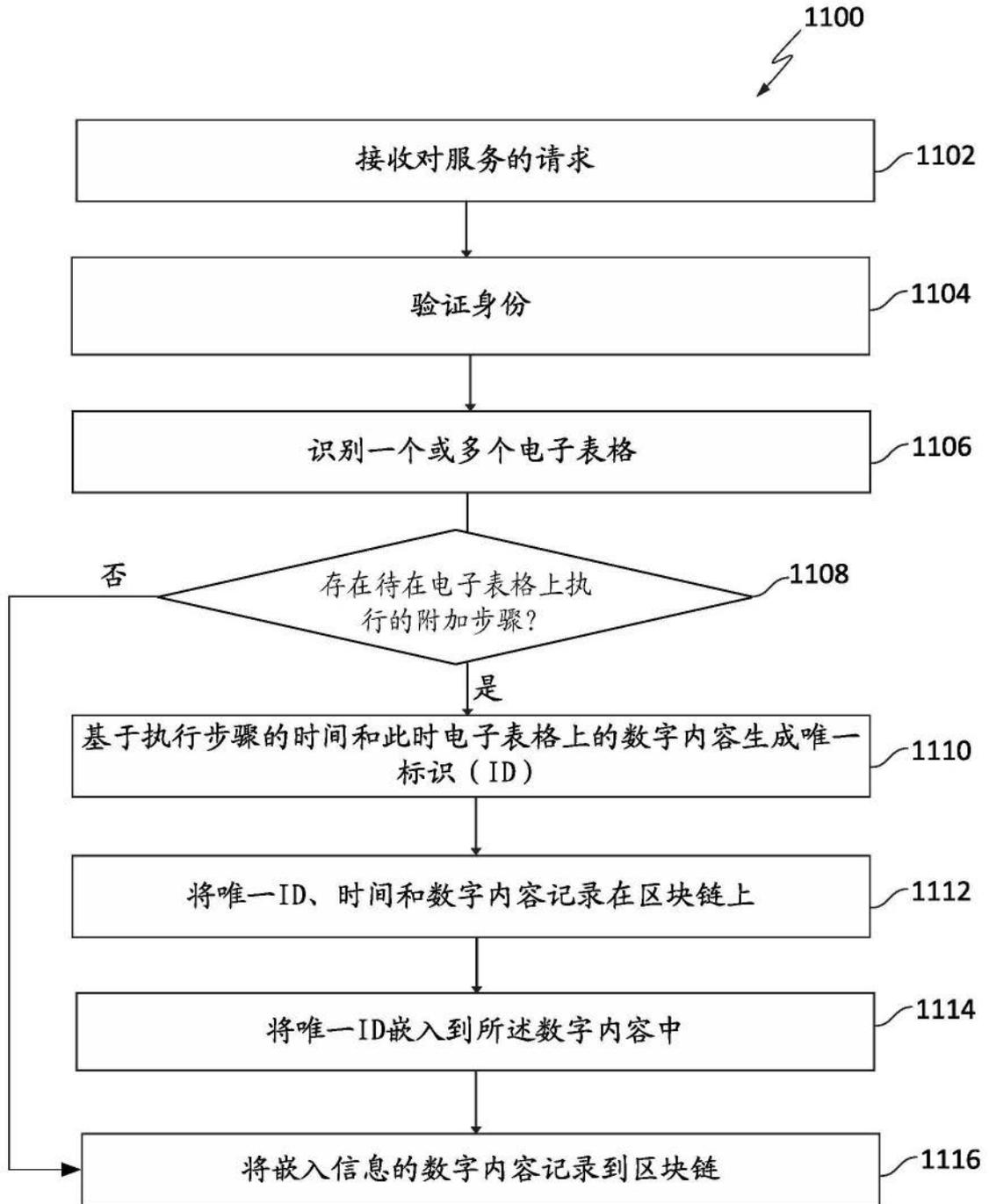


图11

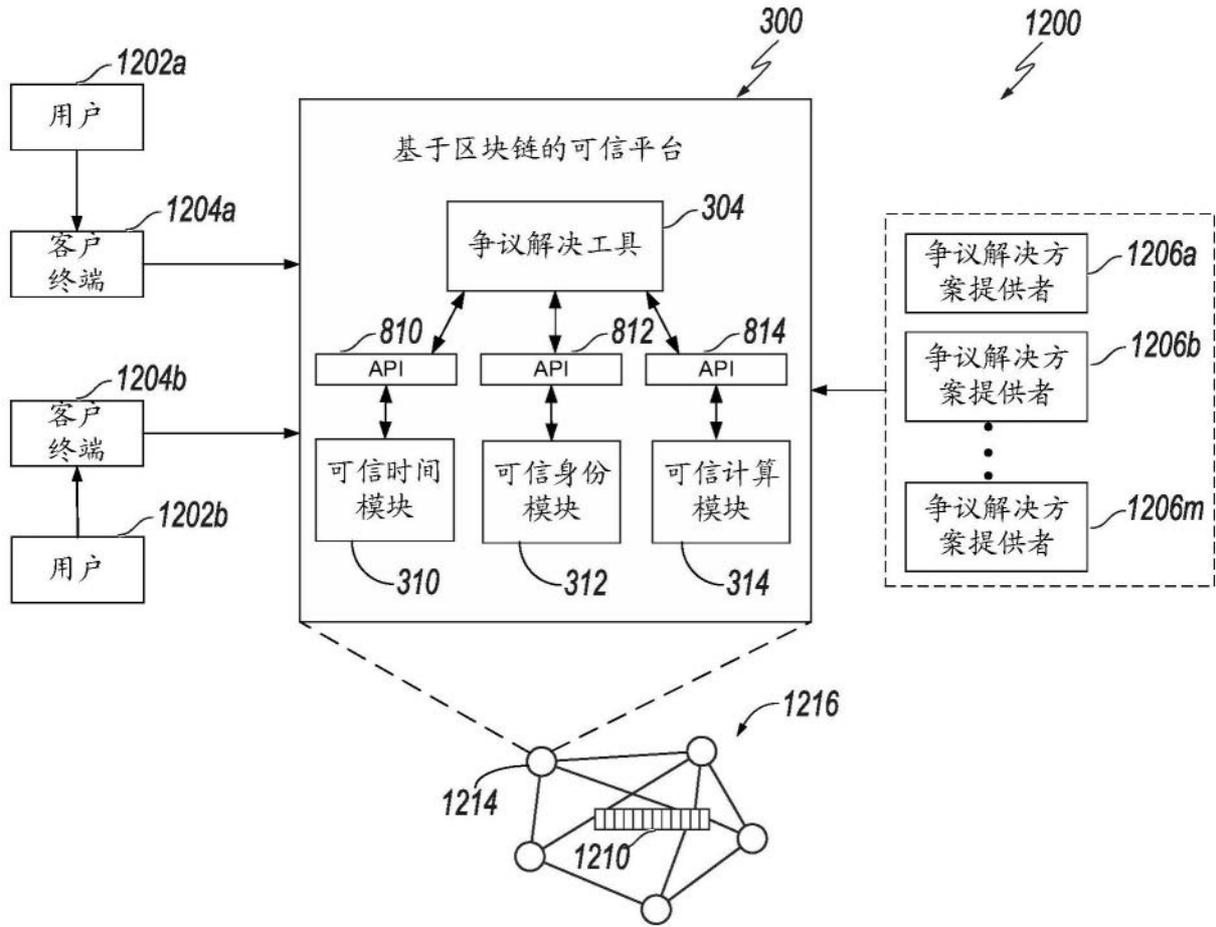


图12

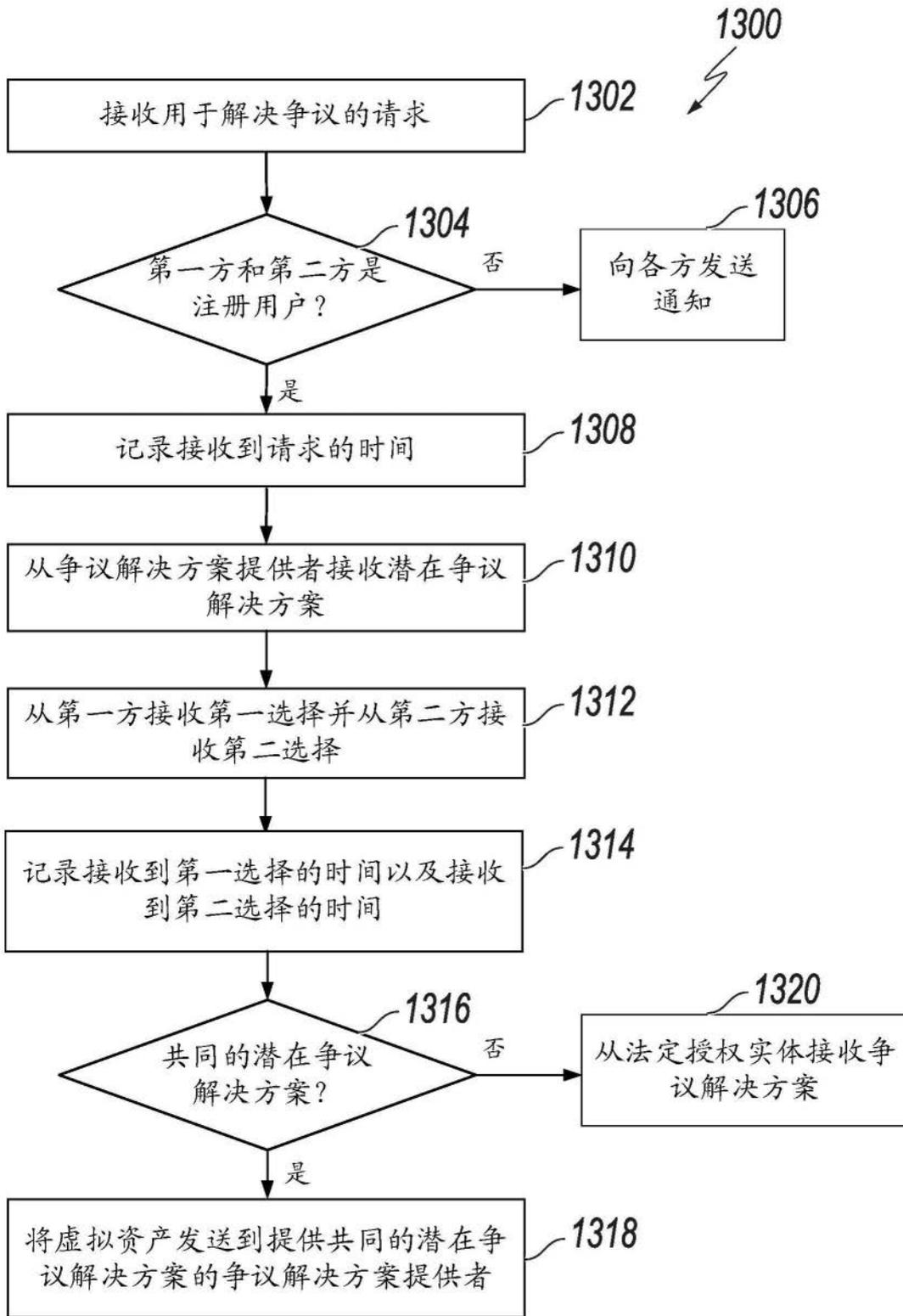


图13

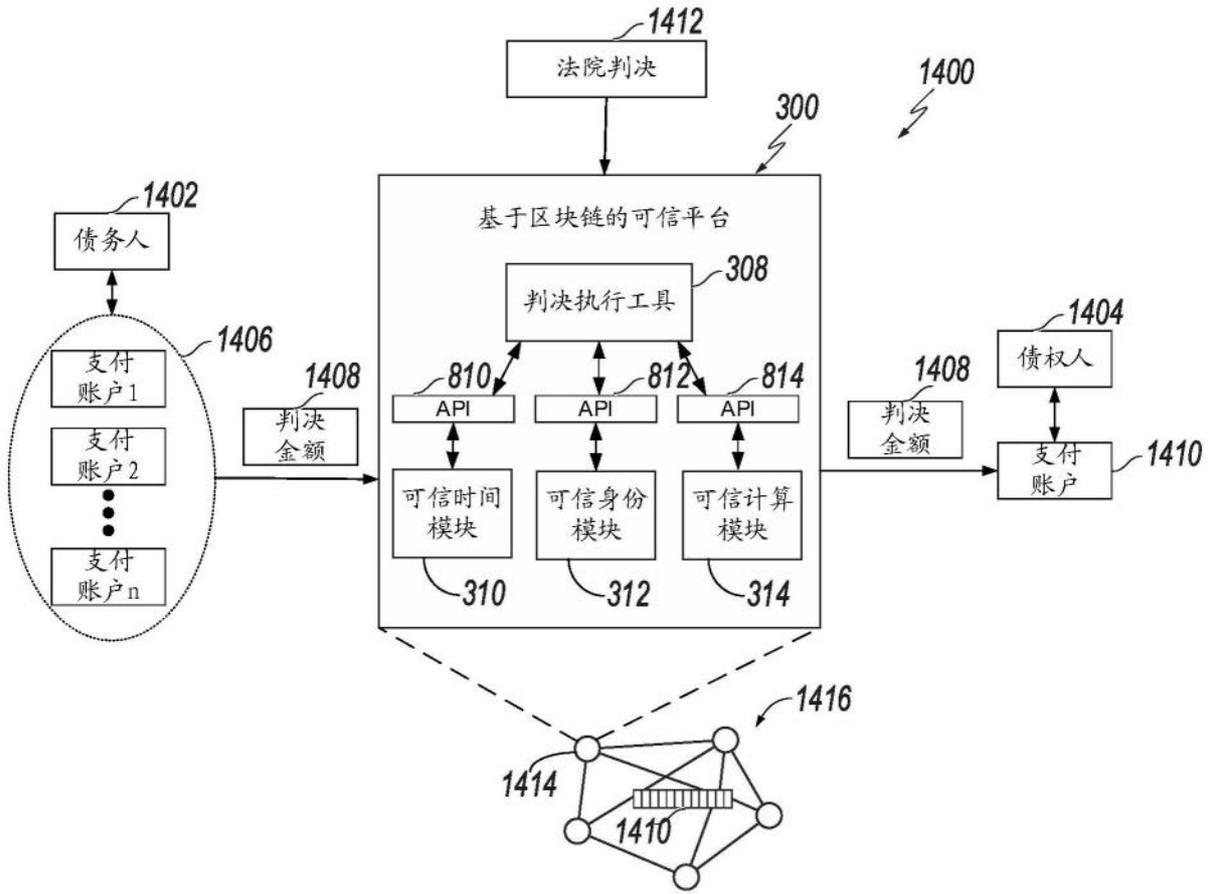


图14

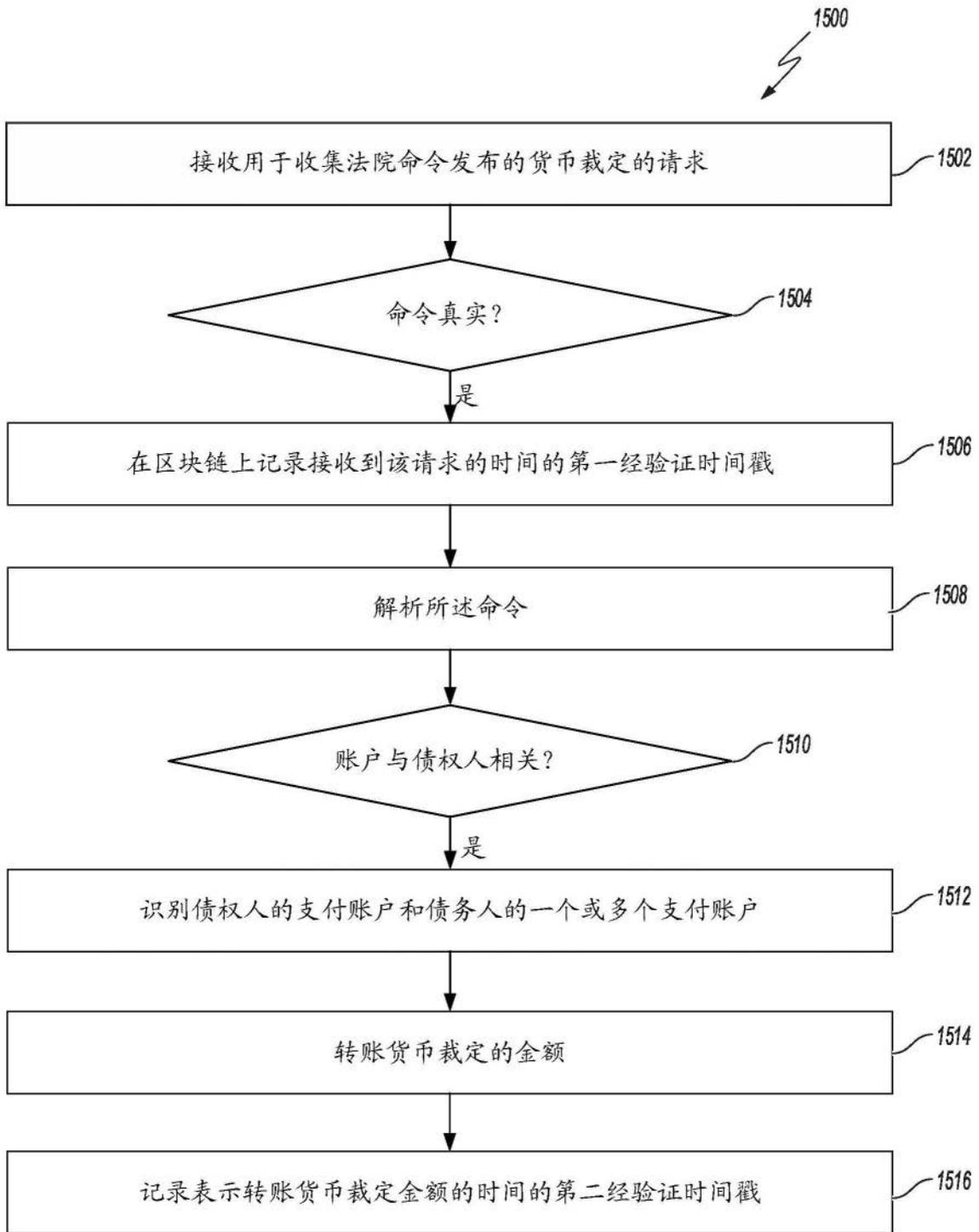


图15

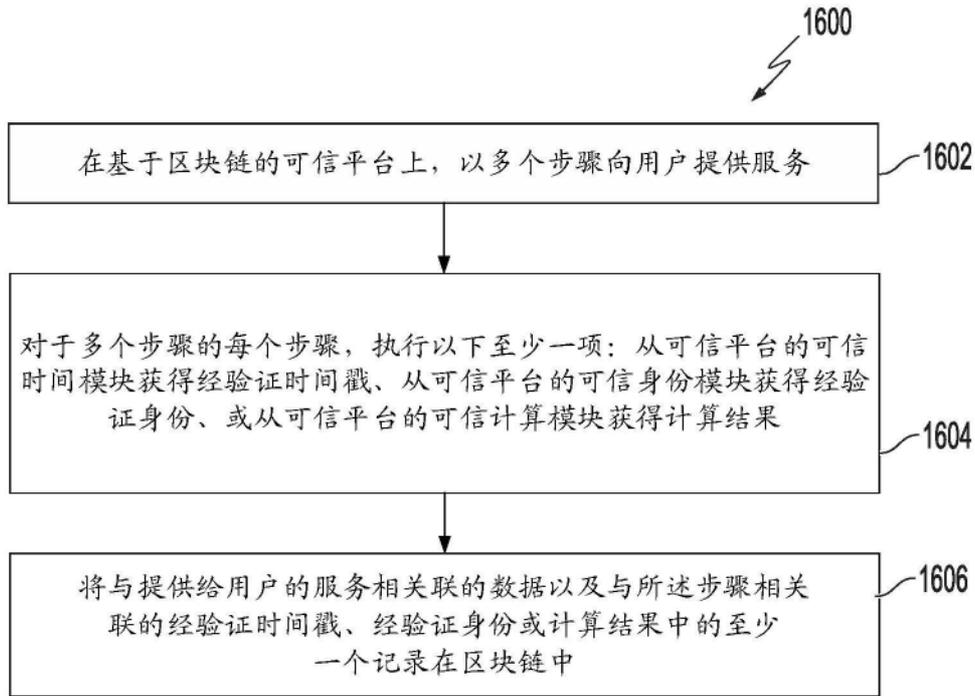


图16

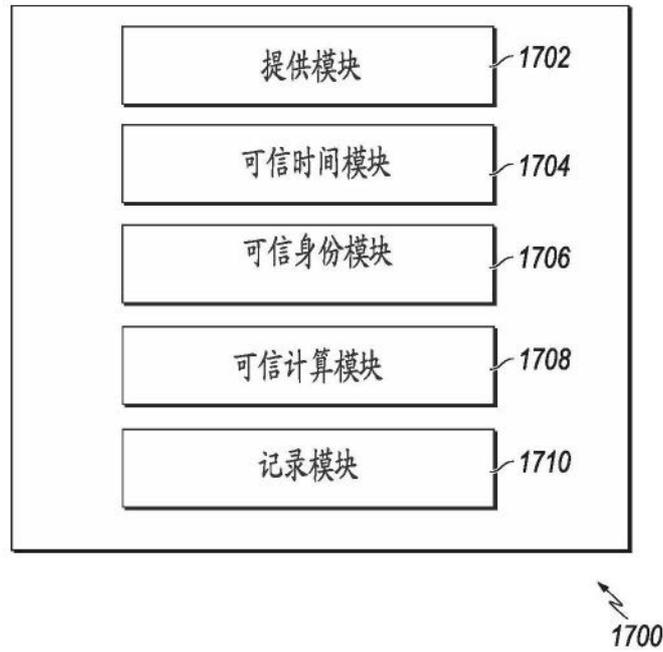


图17

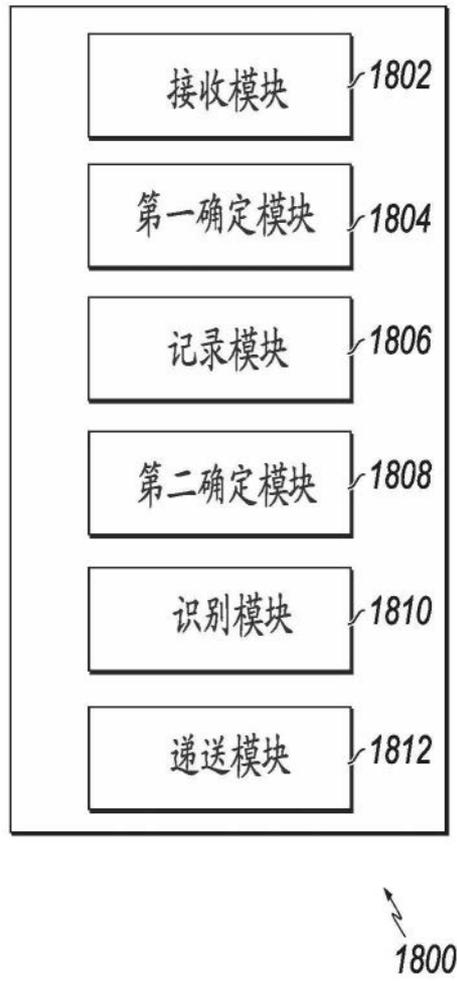


图18

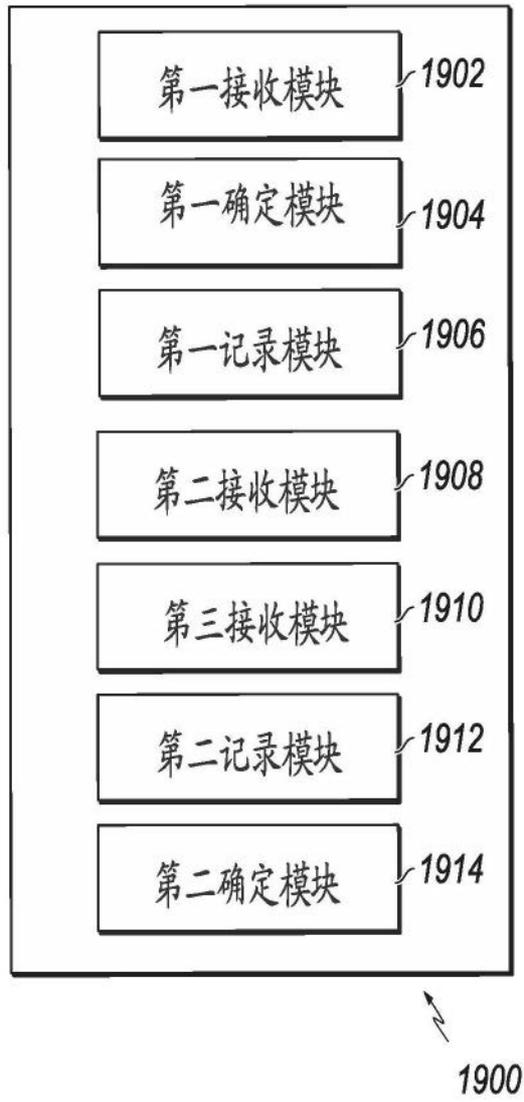


图19

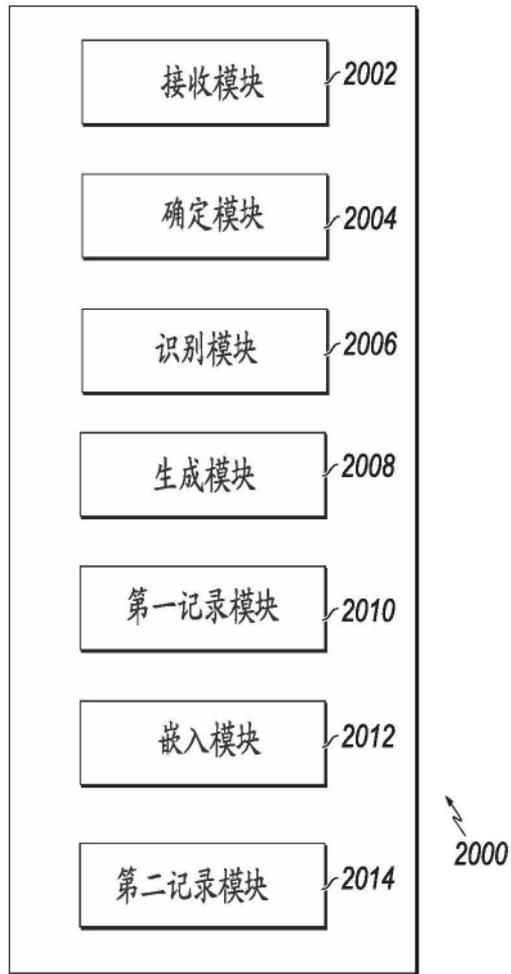


图20

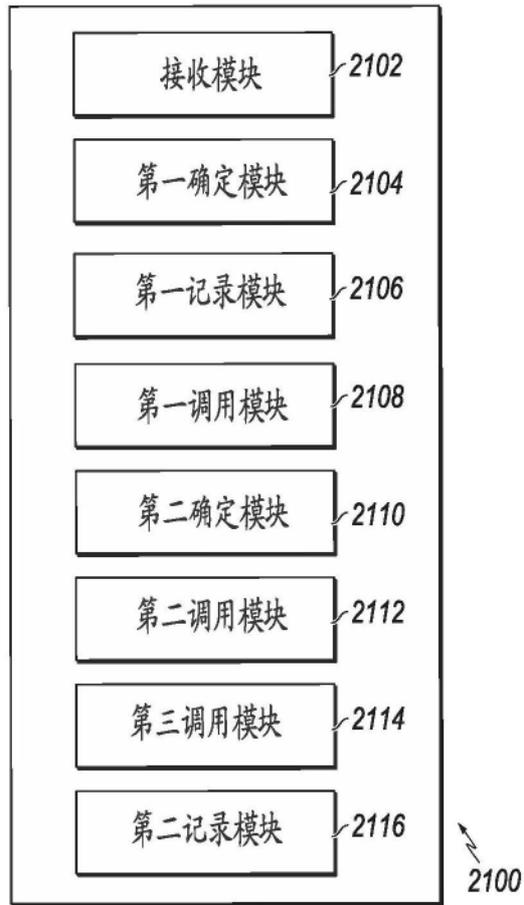


图21