

(12) 按照专利合作条约所公布的国际申请

(19) 世界知识产权组织
国际局

(43) 国际公布日
2018 年 10 月 11 日 (11.10.2018)



(10) 国际公布号
WO 2018/184446 A1

(51) 国际专利分类号:
H04L 9/32 (2006.01) **H04L 29/06** (2006.01)

(21) 国际申请号: PCT/CN2018/078848

(22) 国际申请日: 2018 年 3 月 13 日 (13.03.2018)

(25) 申请语言: 中文

(26) 公布语言: 中文

(30) 优先权:
201710220298.0 2017年4月6日 (06.04.2017) CN

(71) 申请人: 中国移动通信有限公司研究院 (CHINA MOBILE COMMUNICATION LTD., RESEARCH INSTITUTE) [CN/CN]; 中国北京市西城区宣武门西大街 32 号, Beijing 100053 (CN)。中国移动通信集团有限公司

司 (CHINA MOBILE COMMUNICATIONS GROUP CO.,LTD.) [CN/CN]; 中国北京市西城区金融大街29号, Beijing 100032 (CN)。

(72) 发明人: 左敏(ZUO, Min); 中国北京市西城区金融大街29号, Beijing 100032 (CN)。刘福文(LIU, Fuwen); 中国北京市西城区金融大街29号, Beijing 100032 (CN)。阎军智(YAN, Junzhi); 中国北京市西城区金融大街29号, Beijing 100032 (CN)。

(74) 代理人: 北京银龙知识产权代理有限公司(DRAGON INTELLECTUAL PROPERTY LAW FIRM); 中国北京市海淀区西直门北大街32号院枫蓝国际中心2号楼10层, Beijing 100082 (CN)。

(81) 指定国(除另有指明, 要求每一种可提供的国家保护): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG,

(54) Title: METHOD, DEVICE AND SYSTEM FOR REALIZING MUTUAL TRUST BETWEEN CAS, AND ELECTRONIC APPARATUS

(54) 发明名称: 实现CA互信的方法、装置、系统和电子设备

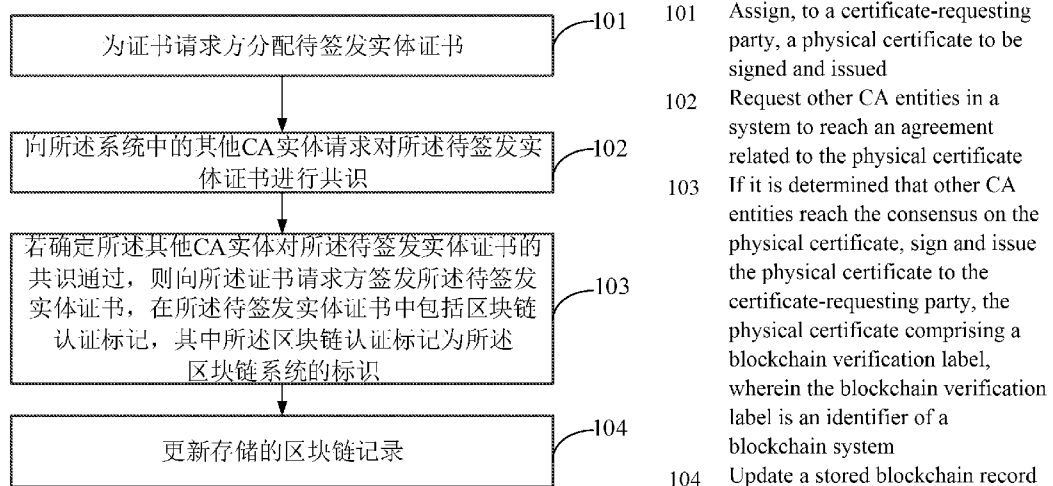


图 1

(57) Abstract: Provided are a method, device and system for realizing mutual trust between CAs, and an electronic apparatus. The method for realizing mutual trust between CAs comprises: assigning, to a certificate-requesting party, a physical certificate to be signed and issued; requesting other CA entities in a system to reach an agreement related to the physical certificate; if it is determined that verification of the physical certificate performed by other CA entities is successful, signing and issuing the physical certificate to the certificate-requesting party, the physical certificate comprising a blockchain verification label, wherein the blockchain verification label is an identifier of a blockchain system; and updating a stored blockchain record.

(57) 摘要: 本公开提供一种实现CA互信的方法、装置、系统和电子设备。本公开的实现CA互信的方法包括: 为证书请求方分配待签发实体证书; 向系统中的其他CA实体请求对待签发实体证书进行共识; 若确定其他CA实体对待签发实体证书的认证通过, 则向证书请求方签发待签发实体证书, 在待签发实体证书中包括区块链认证标记, 其中区块链认证标记为区块链系统的标识; 更新存储的区块链记录。

BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW。

(84) 指定国 (除另有指明, 要求每一种可提供的地区保护): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), 欧亚 (AM, AZ, BY, KG, KZ, RU, TJ, TM), 欧洲 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG)。

本国际公布:

— 包括国际检索报告 (条约第21条(3))。

实现 CA 互信的方法、装置、系统和电子设备

相关申请的交叉引用

本申请主张在 2017 年 4 月 6 日在中国提交的中国专利申请号 No. 201710220298.0 的优先权，其全部内容通过引用包含于此。

技术领域

本公开涉及通信技术领域，尤其涉及一种实现 CA 互信的方法、装置、系统和电子设备。

背景技术

PKI (Public Key Infrastructure, 公钥基础设施) 在信息安全领域扮演着非常重要的角色。无论是使用 HTTPS (Hyper Text Transfer Protocol over Secure Socket Layer, 超文本传输协议安全) 访问安全的网站，还是在数字商务/政务/办公领域经常用到的电子签名，都必须有 PKI 的支撑。

PKI 的依赖方在验证对方证书时，需要构建相应的证书认证路径，而在路径中必须有一个信任起点，即信任锚。信任锚通常是被依赖方信任的 CA (Certificate Authority, 证书权威) 的自签名证书。依赖方的信任锚数量通常是有限的。当对方证书对应的 CA 自签名证书不在依赖方的信任锚范围内时，依赖方就无法构建一个可信的证书认证路径，也就无法完成基于证书的保密通信或签名认证等操作。这就引出了 CA 互信的问题。

在 PKI 实践中，解决 CA 互信问题的方法一般有如下三种：列表方案：常见的权威列表有中华人民共和国工信部《电子认证服务许可证》列表、微软公司 Root Certificate Program 维护的列表（也就是预置在 Windows 操作系统和 IE 浏览器中的 CA 列表）、以及北美 WebTrust 认证的列表等；CA 交叉认证方案（网状结构）：一个 CA 通过为其他 CA 签发证书的方式，使得信任自己的依赖方能与其他 CA 的证书持有者达成互信；以及，桥 CA 方案（星型结构）：引入桥 CA 作为其他 CA 互信的中介，两个 CA 分别与桥 CA 双向交叉认证后，这两个 CA 之间也达成了互信。

但是，在实现本公开的过程中发明人发现列表方案对依赖方有较高要求（有专业的判断能力、能够合理配置自己的信任锚），且权威列表本身的维护代价较高。CA 交叉认证方案类似现实生活中集团平等合作的信任关系。当 CA 数量较少时可以很好地解决 CA 互信问题，但大量 CA 两两进行交叉认证时，就会形成复杂的网状结构，使证书认证路径变长甚至形成环路，而且证书策略（CP）经过多次映射之后会使证书用途大大受限。桥 CA 方案类似现实生活中行业协会中介的信任关系，CA 数量较多时可以避免两两交叉认证的弊端，但桥 CA 运营方的选择是个难题，它的可信程度直接决定了互信关系的可靠程度。

发明内容

有鉴于此，本公开提供一种实现 CA 互信的方法、装置、系统和电子设备，以提高实现 CA 互信的灵活性。

为解决上述技术问题，在第一方面，本公开提供一种实现 CA 互信的方法，该方法应用于 CA 互信系统中的 CA 实体。所述 CA 互信系统包括至少三个 CA 实体，各 CA 实体组成点到点 P2P 网络并形成区块链系统，各 CA 实体中存储有区块链记录，区块链记录用于记录对实体证书的操作记录。所述方法包括：为证书请求方分配待签发实体证书；向所述系统中的其他 CA 实体请求对所述待签发实体证书进行共识；若确定所述其他 CA 实体对所述待签发实体证书的共识通过，则向所述证书请求方签发所述待签发实体证书，在所述待签发实体证书中包括区块链认证标记，其中所述区块链认证标记为所述区块链系统的标识；以及更新存储的区块链记录。

其中，所述各 CA 实体分别对应设置有互信代理，各 CA 实体通过对应设置的互信代理组成 P2P 网络并形成区块链系统；所述区块链记录存储在所述互信代理中。

其中，所述为证书请求方分配待签发实体证书，包括：接收所述证书请求方的证书申请请求；根据所述证书申请请求对所述证书请求方进行身份鉴别，获得所述证书请求方的身份鉴别信息；以及当对所述证书请求方的身份鉴别通过后，为所述证书请求方分配所述待签发实体证书。

其中，所述向所述系统中的其他 CA 实体请求对所述待签发实体证书进行共识，包括：通过对应设置的互信代理，向所述系统中其他 CA 实体对应的互信代理模块请求对所述待签发实体证书进行共识；所述若确定所述其他 CA 实体对所述待签发实体证书的共识通过，则向所述证书请求方签发所述待签发实体证书，包括：若确定所述其他 CA 实体对应的互信代理模块对所述待签发实体证书的共识通过，则向所述证书请求方签发所述待签发实体证书；并且所述更新存储的区块链记录，包括：在所述区块链记录中，增加所述待签发实体证书对应的新增记录。

其中，所述通过对应设置的互信代理，向所述系统中其他 CA 实体对应的互信代理模块请求对所述待签发实体证书进行共识，包括：通过对应设置的互信代理，向所述系统中其他 CA 实体对应的互信代理模块发送所述待签发实体证书、所述证书请求方的身份鉴别信息，以请求对所述待签发实体证书进行共识。

其中，所述 CA 互信系统还包括：各 CA 实体对应的中间 CA 实体；所述向所述证书请求方签发所述待签发实体证书，包括：通过所述中间 CA 实体向所述证书请求方签发所述待签发实体证书。

其中，所述方法还包括：若确定所述其他 CA 实体对所述待签发实体证书的共识未通过，则删除所述待签发实体证书，并向所述证书请求方签发最终实体证书，其中所述最终实体证书中不包括所述区块链认证标记。

其中，在所述为证书请求方分配待签发实体证书的步骤之前，所述方法还包括：接收所述证书请求方的证书更新请求；所述为证书请求方分配待签发实体证书，包括：根据所述证书更新请求，为所述证书请求方分配新的待签发实体证书；所述向所述系统中的其他 CA 实体请求对所述待签发实体证书进行共识，包括：通过对应设置的互信代理，向所述系统中的其他 CA 实体对应的互信代理请求对所述新的待签发实体证书进行共识；所述若确定所述其他 CA 实体对所述待签发实体证书的共识通过，则向所述证书请求方签发所述待签发实体证书，包括：所述若确定所述其他 CA 实体对应的互信代理对所述新的待签发实体证书的共识通过，则向所述证书请求方签发所述新的待签发实体证书；并且所述更新存储的区块链记录，包括：在所述区块链

记录中，增加所述证书请求方的原实体证书对应的更新记录。

其中，所述方法还包括：通知所述其他 CA 实体吊销所述证书请求方的原实体证书。

其中，所述通知所述其他 CA 实体吊销所述证书请求方的原实体证书，包括：通过对应设置的互信代理，向所述其他 CA 实体对应的互信代理发送证书吊销请求，请求吊销所述证书请求方的原实体证书；并且所述更新存储的区块链记录，包括：在所述区块链记录中，增加所述原实体证书对应的吊销记录。

其中，所述方法还包括：接收证书验证请求方的证书验证请求，在所述证书验证请求中包括待验证实体证书；根据所述待验证实体证书确定根 CA 实体，并与所述根 CA 实体交互完成对所述待验证实体证书的验证，获得第一验证结果；确定所述待验证实体证书中是否包含区块链认证标记；若包含所述区块链认证标记，则利用对应设置的互信代理和所述区块链认证标记查找存储的区块链记录，根据查找确定是否通过对所述待验证实体证书的验证，获得第二验证结果；以及，根据所述第一验证结果和所述第二验证结果，向所述证书验证请求方发送最终的验证结果。

其中，所述根据所述第一验证结果和所述第二验证结果，向所述证书验证请求方发送最终的验证结果，包括：若所述第一验证结果和所述第二验证结果均表示通过对所述待验证实体证书的验证，则向所述证书验证请求方发送所述第一验证结果和/或所述第二验证结果；以及若所述第一验证结果和所述第二验证结果不一致，则根据设置的验证结果选择信息，选择优先级较高的验证结果作为最终的验证结果，并向所述证书验证请求方发送所述最终的验证结果。

在第二方面，本公开的一些实施例提供了一种实现 CA 互信的方法，该方法应用于 CA 互信系统中的 CA 实体，所述 CA 互信系统包括至少三个 CA 实体，各 CA 实体组成点到点 P2P 网络并形成区块链系统，各 CA 实体中存储有区块链记录，区块链记录用于记录对实体证书的操作记录。所述方法包括：接收第一 CA 实体的证书共识请求；根据所述第一 CA 实体的证书共识请求，对所述第一 CA 实体的待签发实体证书进行共识，所述待签发实体证

书中包括区块链认证标记，其中所述区块链认证标记为所述区块链系统的标识；以及若确定对所述待签发实体证书的共识通过，则更新存储的区块链记录。

其中，所述更新存储的区块链记录，包括：在所述区块链记录中，增加所述待签发实体证书对应的新增记录。

其中，所述更新存储的区块链记录，还包括：当有实体证书更新时，在所述区块链记录中，增加对进行更新的实体证书对应的更新记录。

其中，所述方法还包括：接收所述第一 CA 实体的证书吊销请求，根据所述证书吊销请求确定是否通过所述证书吊销请求；并且所述更新存储的区块链记录，包括：当通过所述证书吊销请求时，在所述区块链记录中，增加被吊销的实体证书对应的吊销记录。

第三方面，本公开的一些实施例提供了一种实现 CA 互信的装置，该装置应用于 CA 互信系统中的 CA 实体，所述 CA 互信系统包括至少三个 CA 实体，各 CA 实体组成点到点 P2P 网络并形成区块链系统；各 CA 实体中存储有区块链记录，区块链记录用于记录对实体证书的操作记录。所述装置包括：分配模块，用于为证书请求方分配待签发实体证书；请求模块，用于向所述系统中的其他 CA 实体请求对所述待签发实体证书进行共识；签发模块，用于若确定所述其他 CA 实体对所述待签发实体证书的共识通过，则向所述证书请求方签发所述待签发实体证书，在所述待签发实体证书中包括区块链认证标记，其中所述区块链认证标记为所述区块链系统的标识；以及更新模块，用于更新存储的区块链记录。

其中，所述装置还包括：互信代理模块，用于将所述实现 CA 互信的装置与其他 CA 实体组成 P2P 网络并形成区块链系统；所述区块链记录存储在所述互信代理模块中。

其中，所述分配模块包括：接收子模块，用于接收所述证书请求方的证书申请请求；身份鉴别子模块，用于根据所述证书申请请求对所述证书请求方进行身份鉴别，获得所述证书请求方的身份鉴别信息；以及分配子模块，用于当对所述证书请求方的身份鉴别通过后，为所述证书请求方分配所述待签发实体证书。

其中，所述请求模块具体用于，通过对应设置的互信代理模块，向所述系统中其他 CA 实体对应的互信代理模块请求对所述待签发实体证书进行共识；所述签发模块具体用于，若确定所述其他 CA 实体对应的互信代理模块对所述待签发实体证书的共识通过，则向所述证书请求方签发所述待签发实体证书；并且所述更新模块具体用于，在所述区块链记录中，增加所述待签发实体证书对应的新增记录。

其中，所述请求模块具体用于，通过对应设置的互信代理模块，向所述系统中其他 CA 实体对应的互信代理模块发送所述待签发实体证书、所述证书请求方的身份鉴别信息，以请求对所述待签发实体证书进行共识。

其中，所述 CA 互信系统还包括：各 CA 实体对应的中间 CA 实体；并且所述签发模块具体用于，通过所述中间 CA 实体向所述证书请求方签发所述待签发实体证书。

其中，所述装置还包括：删除模块，用于若确定所述其他 CA 实体对所述待签发实体证书的共识未通过，则删除所述待签发实体证书，并向所述证书请求方签发最终实体证书，其中所述最终实体证书中不包括所述区块链认证标记。

其中，所述装置还包括：第一接收模块，用于接收所述证书请求方的证书更新请求；所述分配模块具体用于，根据所述证书更新请求，为所述证书请求方分配新的待签发实体证书；所述请求模块具体用于，通过对应设置的互信代理模块，向所述系统中的其他 CA 实体对应的互信代理模块请求对所述新的待签发实体证书进行共识；所述签发模块具体用于，若确定所述其他 CA 实体对应的互信代理模块对所述新的待签发实体证书的共识通过，则向所述证书请求方签发所述新的待签发实体证书；并且所述更新模块具体用于，在所述区块链记录中，增加所述证书请求方的原实体证书对应的更新记录。

其中，所述装置还包括：通知模块，用于通知所述其他 CA 实体吊销所述证书请求方的原实体证书。

其中，所述通知模块具体用于，通过所述互信代理模块，向所述其他 CA 实体对应的互信代理模块发送证书吊销请求，请求吊销所述证书请求方的原实体证书；并且所述更新模块具体用于，在所述区块链记录中，增加所述原

实体证书对应的吊销记录。

其中，所述装置还包括：第二接收模块，用于接收证书验证请求方的证书验证请求，在所述证书验证请求中包括待验证实体证书；第一验证模块，用于根据所述待验证实体证书确定根 CA 实体，并与所述根 CA 实体交互完成对所述待验证实体证书的验证，获得第一验证结果；第一确定模块，用于确定所述待验证实体证书中是否包含区块链认证标记；第二验证模块，用于若包含所述区块链认证标记，则利用对应设置的互信代理模块和所述区块链认证标记查找存储的区块链记录，根据查找确定是否通过对所述待验证实体证书的验证，获得第二验证结果；以及结果发送模块，用于根据所述第一验证结果和所述第二验证结果，向所述证书验证请求方发送最终的验证结果。

其中，所述结果发送模块具体用于，若所述第一验证结果和所述第二验证结果均表示通过对所述待验证实体证书的验证，则向所述证书验证请求方发送所述第一验证结果和/或所述第二验证结果；以及若所述第一验证结果和所述第二验证结果不一致，则根据设置的验证结果选择信息，选择优先级较高的验证结果作为最终的验证结果，并向所述证书验证请求方发送所述最终的验证结果。

第四方面，本公开的一些实施例提供了一种实现 CA 互信的装置，该装置应用于 CA 互信系统中的 CA 实体，所述 CA 互信系统包括至少三个 CA 实体，各 CA 实体组成点到点 P2P 网络并形成区块链系统，各 CA 实体中存储有区块链记录，区块链记录用于记录对实体证书的操作记录。所述装置包括：接收模块，用于接收第一 CA 实体的证书共识请求；共识模块，用于根据所述第一 CA 实体的证书共识请求，对所述第一 CA 实体的待签发实体证书进行共识，所述待签发实体证书中包括区块链认证标记，其中所述区块链认证标记为所述区块链系统的标识；以及更新模块，用于若确定对所述待签发实体证书的共识通过，则更新存储的区块链记录。

其中，所述更新模块具体用于，在所述区块链记录中，增加所述待签发实体证书对应的新增记录。

其中，所述更新模块具体用于，当有实体证书更新时，在所述区块链记录中，增加对进行更新的实体证书对应的更新记录。

其中，所述接收模块还用于，接收所述第一 CA 实体的证书吊销请求，根据所述证书吊销请求确定是否通过所述证书吊销请求；并且所述更新模块具体用于，当通过所述证书吊销请求时，在所述区块链记录中，增加被吊销的实体证书对应的吊销记录。

第五方面，本公开的一些实施例提供了一种实现 CA 互信的系统，包括：至少三个 CA 实体，各 CA 实体组成点到点 P2P 网络并形成区块链系统；各 CA 实体中存储有区块链记录，用于记录对实体证书的操作记录；其中，所述至少三个 CA 实体中的第一 CA 实体，为证书请求方分配待签发实体证书，并向所述系统中的第二 CA 实体请求对所述待签发实体证书进行共识；若确定所述第二 CA 实体对所述待签发实体证书的共识通过，则向所述证书请求方签发所述待签发实体证书，在所述待签发实体证书中包括区块链认证标记，其中所述区块链认证标记为所述区块链系统的标识，并更新存储的区块链记录；并且所述至少三个 CA 实体中的第二 CA 实体，接收所述第一 CA 实体的证书共识请求，并根据所述第一 CA 实体的证书共识请求，对所述第一 CA 实体的待签发实体证书进行共识，若确定对所述待签发实体证书的共识通过，则更新存储的区块链记录。

其中，所述各 CA 实体分别对应设置有互信代理，各 CA 实体通过对应设置的互信代理组成 P2P 网络并形成区块链系统；所述区块链记录存储在所述互信代理中。

第六方面，本公开的一些实施例提供了一种电子设备，包括：处理器，存储器，用于存储计算机程序；其中，所述处理器在调用并执行所述存储器上存储的计算机程序时，所述处理器实现如前述第一方面所述的实现证书权威 CA 互信的方法。

第七方面，本公开的一些实施例提供了一种计算机可读存储介质，包括在所述计算机可读存储介质上存储的计算机程序，其中，当所述计算机程序被处理器执行时，所述处理器执行如前述第一方面所述的实现证书权威 CA 互信的方法。

第八方面，本公开的一些实施例提供了一种电子设备，包括处理器，存储器，用于存储计算机程序；其中，所述处理器在调用并执行所述存储器上

存储的计算机程序时，所述处理器实现如前述第二方面所述的实现证书权威 CA 互信的方法。

第九方面，本公开的一些实施例提供了一种计算机可读存储介质，包括在所述计算机可读存储介质上存储的计算机程序，其中，当所述计算机程序被处理器执行时，所述处理器执行如前述第二方面所述的实现证书权威 CA 互信的方法。

本公开的上述技术方案的有益效果如下：

在本公开的一些实施例中，在区块链系统中，可实现基于区块链认证标记进行证书的相关处理，无需复杂的网状交叉认证，无需依靠公信力更高的权威中介建立桥接关系，即可实现每个用户证书粒度的精细互信控制。因此，利用本公开的一些实施例的方案，提高了实现 CA 互信的灵活性。

附图说明

图 1 为本公开的一些实施例的实现 CA 互信的方法的流程图；
图 2 为本公开的一些实施例的实现 CA 互信的方法的流程图；
图 3 为本公开的一些实施例的实现 CA 互信的系统的示意图；
图 4 为本公开的一些实施例的证书注册流程的流程图；
图 5 为本公开的一些实施例的区块链的结构示意图；
图 6 为本公开的一些实施例的证书更新流程的流程图；
图 7 为本公开的一些实施例的证书吊销流程的流程图；
图 8 为本公开的一些实施例的证书查询流程的流程图；
图 9 为本公开的一些实施例的实现 CA 互信的装置的示意图；
图 10 为本公开的一些实施例的实现 CA 互信的装置的结构图；
图 11 为本公开的一些实施例的实现 CA 互信的装置的示意图；以及
图 12 为本公开的一些实施例的电子设备的示意图。

具体实施方式

下面将结合附图和实施例，对本公开的具体实施方式作进一步详细描述。以下实施例用于说明本公开，但不用来限制本公开的范围。

如图 1 所示, 本公开的一些实施例的实现 CA 互信的方法, 应用于 CA (Certificate Authority, 证书权威) 互信系统中的 CA 实体。所述 CA 互信系统包括: 至少三个 CA 实体, 各 CA 实体组成点到点 P2P 网络并形成区块链系统; 各 CA 实体中存储有区块链记录, 用于记录对实体证书的操作记录。所述方法包括步骤 101-104。

步骤 101、为证书请求方分配待签发实体证书。

步骤 102、向所述系统中的其他 CA 实体请求对所述待签发实体证书进行共识。

步骤 103、若确定所述其他 CA 实体对所述待签发实体证书的共识通过, 则向所述证书请求方签发所述待签发实体证书, 在所述待签发实体证书中包括区块链认证标记, 其中所述区块链认证标记为所述区块链系统的标识。

步骤 104、更新存储的区块链记录。

在实际应用中, 所述各 CA 实体分别对应设置有互信代理, 各 CA 实体通过对应设置的互信代理组成 P2P 网络并形成区块链系统; 所述区块链记录存储在所述互信代理中。而各 CA 实体之间的通信, 是通过各 CA 实体对应设置的互信代理完成的。

在本公开的一些实施例中, 在区块链系统中, 可实现基于区块链认证标记进行证书的相关处理, 无需复杂的网状交叉认证, 无需依靠公信力更高的权威中介建立桥接关系, 即可实现每用户证书粒度的精细互信控制。因此, 利用本公开的一些实施例的方案, 提高了实现 CA 互信的灵活性。

如图 2 所示, 本公开的一些实施例的实现 CA 互信的方法, 应用于 CA 互信系统中的 CA 实体; 所述 CA 互信系统包括: 至少三个 CA 实体, 各 CA 实体组成点到点 P2P 网络并形成区块链系统; 各 CA 实体中存储有区块链记录, 用于记录对实体证书的操作记录。所述方法包括步骤 201-203。

步骤 201、接收第一 CA 实体的证书共识请求。

步骤 202、根据所述第一 CA 实体的证书共识请求, 对所述第一 CA 实体的待签发实体证书进行共识, 在所述待签发实体证书中包括区块链认证标记, 其中所述区块链认证标记为所述区块链系统的标识。

步骤 203、若确定对所述待签发实体证书的共识通过, 则更新存储的区

块链记录。

其中，所述第一 CA 实体为 CA 互信系统中其他的任意一个 CA 实体。

在本公开的一些实施例中，在区块链系统中，可实现基于区块链认证标记进行证书的相关处理，无需复杂的网状交叉认证，无需依靠公信力更高的权威中介建立桥接关系，即可实现每用户证书粒度的精细互信控制。因此，利用本公开的一些实施例的方案，提高了实现 CA 互信的灵活性。

如图 3 所示，本公开的一些实施例的实现 CA 互信的系统包括：至少三个 CA 实体 301，各 CA 实体组成点到点 P2P 网络并形成区块链系统；各 CA 实体中存储有区块链记录，用于记录对实体证书的操作记录。

其中，所述至少三个 CA 实体中的第一 CA 实体，为证书请求方分配待签发实体证书，并向所述系统中的第二 CA 实体请求对所述待签发实体证书进行共识；若确定所述第二 CA 实体对所述待签发实体证书的共识通过，则向所述证书请求方签发所述待签发实体证书，在所述待签发实体证书中包括区块链认证标记，其中所述区块链认证标记为所述区块链系统的标识，并更新存储的区块链记录；

所述至少三个 CA 实体中的第二 CA 实体，接收所述第一 CA 实体的证书共识请求，并根据所述第一 CA 实体的证书共识请求，对所述第一 CA 实体的待签发实体证书进行共识，若确定对所述待签发实体证书的共识通过，则更新存储的区块链记录。

在实际应用中，所述各 CA 实体分别对应设置有互信代理 302，各 CA 实体通过对应设置的互信代理组成 P2P 网络并形成区块链系统；所述区块链记录存储在所述互信代理中。

每个 CA 实体为传统 PKI 系统中的证书权威。每个 CA 拥有一定数量的依赖方，这些依赖方将该 CA 的自签名证书作为自己的信任锚。该系统中 CA 的数量应为 3 个以上。其中，每个 CA 可有多个二级 CA，每个 CA 可以签发若干个二级 CA 证书，每个二级 CA 又可以签发若干个最终实体证书，从而构成以 CA 自签名证书为根的证书链。常见的证书链长度一般是 3 级，但也可以少于或多于 3 级。

在图 3 中，证书实体（可作为证书请求方、证书验证请求方等角色）为

最终实体证书的拥有者，其身份真实性由为其颁发最终实体证书的 CA 担保。证书依赖方为最终实体证书的验证者。每个证书依赖方可以选择一个或多个信任的 CA，并将其自签名证书作为自己的信任锚。只有能够链接到某个信任锚的最终实体证书，才可以被依赖方直接验证。无法链接到信任锚的最终实体证书，只能通过 CA 互信机制才可被依赖方验证。

以下，结合不同的过程来描述一下本公开的一些实施例的实现过程，包括：1) 证书注册流程；2) 证书更新流程；3) 证书吊销流程；4) 证书使用查询流程。

如图 4 所示，本公开的一些实施例的证书注册流程包括步骤 401-407。

步骤 401、证书实体 1 向选定的 CA1 提交证书申请请求。

在此，证书实体 1 作为证书请求方，在本地生成公私钥对，并将公钥、身份信息及一些辅助信息写入 CSR (Certificate Signing Request, 证书签名请求) 请求，并用私钥对 CSR 请求进行签名，最后将带有签名的 CSR 请求发送给 CA 指定的注册权威 (RA)。

步骤 402、CA1 根据证书策略 (CP) 和认证业务声明 (CPS) 中的约定，对证书实体 1 进行身份鉴别，并保存身份鉴别的证据 (即证书实体 1 的身份鉴别信息)。

其中，CA 在进行身份鉴别时可以采用很多种方法，如要求申请者 (证书实体) 提供相关证明文件、或接受电话访谈、或点击一封确认邮件中的某个链接等等。具体采用何种形式，由 CPS 来约定。

步骤 403、若身份鉴别无误，则 CA1 为证书实体 1 分配一个待签发的实体证书，该待签发的实体证书中包含了区块链认证标记，并通过互信代理 1 将上述待签发的实体证书、以及在身份鉴别过程中获取的证据 (经过电子化处理) 一并发给区块链系统中其它 CA 的互信代理，请求对该新增证书达成共识。

其中，区块链认证标记可以是用于区分不同区块链系统的一个 ID，形如 CA_alliance_cn，由区块链系统自己约定，CA 实体的互信代理在加入区块链系统的时候会获知这个 ID。这个标记可以作为一个证书扩展项存在，因此不会造成与传统证书的不兼容，不支持该证书扩展项的依赖方可以忽略不予处

理。

步骤 404、区块链系统中其它 CA 的互信代理收到 CA1 的共识请求后，根据预先设定的规则（例如根据自己 CP、CPS 编写的智能合约）判断是否接受 CA1 对证书实体 1 的身份鉴别结论、以及验证 CA1 为证书实体 1 签发的证书本身是否有误。

在本公开的一些实施例的系统中，区块链系统由代表根 CA 的互信代理组成。一个根 CA 下面可以有 CP/CPS 互异的多个二级 CA，并分别签发不同类型的证书。互信代理负责进行 CP/CPS 映射和身份鉴别证据的审查，这个过程可以用智能合约来完成。

步骤 405、区块链系统中所有 CA 的互信代理通过某种预先约定的“共识机制”达成集体决议。若共识成功，则该新增证书被追加到区块链中，并在区块链系统中生成一条新的“新增证书记录”，被所有 CA 的互信代理保存。若共识失败，则该新增证书被区块链系统放弃。只有通过了系统中所有 CA 共识的那些证书才被区块链包含，所以可以说本公开的一些实施例的方案是一个“per 用户证书（每个用户证书）”的互信方案。

其中，各 CA 可能采用的区块链“共识机制”包括但不限于：1）拜占庭算法；2）工作量证明；3）权益证明等。

如图 5 所示为区块链的结构示意图。为了方便证书查询，在一定时间单位内生成的证书可放入同一区块，例如可以 24 小时为时间单位。

步骤 406、若上述包含了区块链认证标记的待签发实体证书在区块链系统中共识成功，则 CA1 将通知证书实体 1 下载该证书，或者直接将该证书发送给证书实体 1。

步骤 407、若共识失败，则 CA1 删除上述包含了区块链认证标记的待签发实体证书，重新为证书实体 1 签发不包含区块链认证标记的实体证书，并通知证书实体 1 下载该证书，或者直接将该证书发送给证书实体 1。

其中，为保护 CA1 的自签名证书私钥，通常通过 1 个或多个中间 CA 进行证书的签发。最终下载或发送实体证书时，除了 CA1 签发的证书之外，还可能包括中间 CA 的证书。

最后，证书实体 1 将收到的证书与对应的私钥一起安全存储在本地备用。

如图 6 所示，本公开的一些实施例的证书更新流程包括步骤 601-605。

步骤 601、证书实体 1 向 CA1 提交证书更新请求。

其中，证书实体 1 需要生成新的公私钥对。证书实体 1 所提交的证书更新请求，指的是针对包含了区块链认证标记的最终实体证书的证书更新请求。

步骤 602、CA1 为证书实体 1 分配新的包含了区块链认证标记的待签发实体证书，并通过互信代理 1 将上述证书及相关辅助信息发给区块链系统中其它 CA 的互信代理，请求对更新证书达成共识。

步骤 603、区块链系统中其它 CA 的互信代理收到 CA1 的共识请求后，根据预先设定的规则判断是否接受这条证书更新记录。

区块链系统中所有 CA 的互信代理通过预先约定的“共识机制”达成集体决议。

步骤 604、若共识成功，则该证书更新记录被追加到区块链中，生成一条新的“证书更新记录”，被所有 CA 的互信代理保存。该证书更新记录用于记录证书实体 1 的原有证书被更新。若共识失败，则该证书的更新记录被区块链系统放弃。

步骤 605、若上述证书更新记录在区块链系统中共识成功，则 CA1 将该新的待签发证书返回给证书实体 1。若共识失败，则 CA1 删除上述新的待签发证书，重新为证书实体 1 签发不包含区块链认证标记的最终实体证书，并将其返回给证书实体 1。同时，CA1 发起一次证书吊销流程（下文详细描述），通知系统中其它 CA 将区块链中的旧证书吊销。

在上述过程中，系统中存在两种不同的最终实体证书，一种包含区块链认证标记，另一种不包含区块链认证标记。这是为了实现“per 用户证书”的互信。如果区块链中的其他 CA 不认同 CA1 提供的身份鉴别结果（根据鉴别证据和各自的 CP/CPS 来判断），这个证书就不能写入区块链。

最后，证书实体 1 将收到的证书与对应的私钥一起，安全存储在本地备用。

其中，上述证书更新过程可以独立实现，也可结合证书注册过程实现。

如图 7 所示，本公开的一些实施例的证书吊销流程包括步骤 701-704。

步骤 701、证书实体 1 向 CA1 提交证书吊销申请（主动吊销），或 CA1

单方面决定吊销证书实体 1 的证书（被动吊销）。

此处仅考虑包含了区块链认证标记的最终实体证书。

步骤 702、CA1 通过互信代理 1 发送证书吊销请求，将证书吊销记录发给区块链系统中其它 CA 的互信代理，请求对吊销证书达成共识。

步骤 703、区块链系统中其它 CA 的互信代理收到 CA1 的共识请求后，根据预先设定的规则判断是否接受这条证书吊销记录。

为了及时应对私钥泄露等安全事件，证书吊销请求应具有最高优先级，因此系统中的每个 CA 应设定适当的规则，确保吊销请求能够快速达成共识。

步骤 704、区块链系统中所有 CA 的互信代理通过预先约定的“共识机制”达成集体决议。共识成功后该证书吊销记录被追加到区块链中。

具体的，在所述区块链记录中，增加证书实体 1 的原实体证书对应的吊销记录。

若共识失败，CA1 可在本身的证书状态记录（可与区块链相同，或者不同）中，增加证书实体 1 的原实体证书对应的吊销记录。

如图 8 所示，本公开的一些实施例的证书查询流程包括步骤 801-805。

步骤 801、证书实体 1 与证书依赖方 1 建立通信关系，证书实体 1 向证书依赖方 1 出示自己的最终实体证书（可能还包含相应中间 CA 的证书），例如用于加密通信或数字签名。

步骤 802、证书依赖方 1 需要验证证书实体 1 出示的最终实体证书是否真实有效。证书依赖方 1 尝试重建该证书的完整证书链，发现该证书链的根是 CA1，而 CA1 并不是证书依赖方 1 的信任锚。

步骤 803、证书依赖方 1 向自己的信任锚 CA5 发送证书验证请求，请求中携带证书实体 1 出示的最终实体证书。

步骤 804、CA5 收到证书验证请求后，进行验证。其中，（1）、（2）两种方式不分先后。

（1）尝试重建该证书的完整证书链，发现该证书链的根是 CA1。接着检查是否与 CA1 存在传统的交叉认证、桥认证关系。若存在，则按照传统的方法校证书链。同时，获得第一验证结果。

（2）检查该最终实体证书中是否包含区块链认证标记。若包含，则执行

如下操作：

CA5 通过互信代理 5 在区块链中查询关于该最终实体证书的所有记录，包括新增、更新、吊销等。互信代理 5 根据查询结果判断该证书是否被自己共识过，以及是否仍然有效。这个判断过程仅凭查询到的记录即可完成，无需再重建和验证整个证书链。同时，获得第二验证结果。

步骤 805、CA5 向证书依赖方 1 发送验证结果。

在具体实现过程中，为了兼容传统的 PKI 互信体系，允许为传统互信体系和区块链互信体系设置不同的优先级；有些证书不带有区块链认证标识，无法在区块链上查询到，只能依靠传统的互信体系。

若步骤 804 中的两种方法均无法完成证书验证，则 CA5 返回给证书依赖方 1 一个“无法验证”的响应。若只有一种方法可以完成证书验证，或两种方法均可完成验证且验证结果一致，则直接将该任意一个或者两个验证结果返回给证书依赖方 1。若两种方法均可完成验证但验证结果不一致，则按照 CA5 预定的规则，取优先级较高的一种方法，将其验证结果返回给证书依赖方 1。

证书依赖方 1 收到来自 CA5 的验证结果，根据验证结果决定是否继续执行与证书实体 1 之间的通信过程（如建立加密通信关系，或验证证书实体 1 的数字签名）。

上述一些流程合在一起，可实现区块链系统中所有 CA 信任域的全面融合。系统中的 CA 无需再进行复杂的交叉认证，也无需另一个公信力更高的机构来建立一个桥 CA。同时，可实现 per 用户证书粒度的精细互信控制，即，其它 CA 无需信任 CA1 签发的所有最终实体证书，它们可以选择只信任能够在区块链中达成共识的证书（包含了区块链认证标记的证书）。需要说明的是，在实际应用中，上述几个流程可以结合使用，也可单独使用。

在本公开的一些实施例中，在区块链系统中，可实现基于区块链认证标记进行证书的相关处理，无需复杂的网状交叉认证，无需依靠公信力更高的权威中介建立桥接关系，即可实现每用户证书粒度的精细互信控制。因此，利用本公开的一些实施例的方案，提高了实现 CA 互信的灵活性。

如图 9 所示，本公开的一些实施例的实现 CA 互信的装置，应用于 CA

互信系统中的 CA 实体；所述 CA 互信系统包括：至少三个 CA 实体，各 CA 实体组成点到点 P2P 网络并形成区块链系统；各 CA 实体中存储有区块链记录，用于记录对实体证书的操作记录；所述装置包括：分配模块 901，用于为证书请求方分配待签发实体证书；请求模块 902，用于向所述系统中的其他 CA 实体请求对所述待签发实体证书进行共识；签发模块 903，用于若确定所述其他 CA 实体对所述待签发实体证书的共识通过，则向所述证书请求方签发所述待签发实体证书，在所述待签发实体证书中包括区块链认证标记，其中所述区块链认证标记为所述区块链系统的标识；和更新模块 904，用于更新存储的区块链记录。

如图 10 所示，所述装置还包括：互信代理模块 905，用于将所述实现 CA 互信的装置与其他 CA 实体组成 P2P 网络并形成区块链系统；所述区块链记录存储在所述互信代理模块中。

其中，所述分配模块 901 包括：接收子模块，用于接收所述证书请求方的证书申请请求；身份鉴别子模块，用于根据所述证书申请请求对所述证书请求方进行身份鉴别，获得所述证书请求方的身份鉴别信息；分配子模块，用于当对所述证书请求方的身份鉴别通过后，为所述证书请求方分配所述待签发实体证书。

其中，所述请求模块 902 具体用于，通过对应设置的互信代理模块，向所述系统中其他 CA 实体对应的互信代理模块请求对所述待签发实体证书进行共识；所述签发模块 903 具体用于，若确定所述其他 CA 实体对应的互信代理模块对所述待签发实体证书的共识通过，则向所述证书请求方签发所述待签发实体证书；所述更新模块 904 具体用于，在所述区块链记录中，增加所述待签发实体证书对应的新增记录。

在一个实施例中，所述请求模块 902 具体用于，通过对应设置的互信代理模块，向所述系统中其他 CA 实体对应的互信代理模块发送所述待签发实体证书、所述证书请求方的身份鉴别信息，以请求对所述待签发实体证书进行共识。

在实际应用中，所述 CA 互信系统还包括：各 CA 实体对应的中间 CA 实体；所述签发模块具体用于，通过所述中间 CA 实体向所述证书请求方签发

所述待签发实体证书。

再如图 10 所示, 所述装置还包括: 删除模块 906, 用于若确定所述其他 CA 实体对所述待签发实体证书的共识未通过, 则删除所述待签发实体证书, 并向所述证书请求方签发最终实体证书, 其中所述最终实体证书中不包括所述区块链认证标记; 以及第一接收模块 907, 用于接收所述证书请求方的证书更新请求。此时, 所述分配模块 901 具体用于, 根据所述证书更新请求, 为所述证书请求方分配新的待签发实体证书; 所述请求模块 902 具体用于, 通过对应设置的互信代理模块, 向所述系统中的其他 CA 实体对应的互信代理模块请求对所述新的待签发实体证书进行共识; 所述签发模块 903 具体用于, 若确定所述其他 CA 实体对应的互信代理模块对所述新的待签发实体证书的共识通过, 则向所述证书请求方签发所述新的待签发实体证书; 所述更新模块 904 具体用于, 在所述区块链记录中, 增加所述证书请求方的原实体证书对应的更新记录。

再如图 10 所示, 所述装置还包括: 通知模块 908, 用于通知所述其他 CA 实体吊销所述证书请求方的原实体证书。

具体的, 所述通知模块 908 具体用于, 通过所述互信代理模块, 向所述其他 CA 实体对应的互信代理模块发送证书吊销请求, 请求吊销所述证书请求方的原实体证书; 所述更新模块 904 具体用于, 在所述区块链记录中, 增加所述原实体证书对应的吊销记录。

再如图 10 所示, 所述装置还包括: 第二接收模块 909, 用于接收证书验证请求方的证书验证请求, 在所述证书验证请求中包括待验证实体证书; 第一验证模块 910, 用于根据所述待验证实体证书确定根 CA 实体, 并与所述根 CA 实体交互完成对所述待验证实体证书的验证, 获得第一验证结果; 第一确定模块 911, 用于确定所述待验证实体证书中是否包含区块链认证标记; 第二验证模块 912, 用于若包含所述区块链认证标记, 则利用对应设置的互信代理模块和所述区块链认证标记查找存储的区块链记录, 根据查找确定是否通过对所述待验证实体证书的验证, 获得第二验证结果; 结果发送模块 913, 用于根据所述第一验证结果和所述第二验证结果, 向所述证书验证请求方发送最终的验证结果。

其中，所述结果发送模块 913 具体用于，若所述第一验证结果和所述第二验证结果均表示通过对所述待验证实体证书的验证，则向所述证书验证请求方发送所述第一验证结果和/或所述第二验证结果；若所述第一验证结果和所述第二验证结果不一致，则根据设置的验证结果选择信息，选择优先级较高的验证结果作为最终的验证结果，并向所述证书验证请求方发送所述最终的验证结果。

本公开所述装置的工作原理可参照前述方法实施例的描述。

在本公开的一些实施例中，可实现基于区块链认证标记进行证书的相关处理，无需复杂的网状交叉认证，无需依靠公信力更高的权威中介建立桥接关系，即可实现每用户证书粒度的精细互信控制。因此，利用本公开的一些实施例的方案，提高了实现 CA 互信的灵活性。

如图 11 所示，本公开的一些实施例的实现 CA 互信的装置，应用于 CA 互信系统中的 CA 实体；所述 CA 互信系统包括：至少三个 CA 实体，各 CA 实体组成点到点 P2P 网络并形成区块链系统；各 CA 实体中存储有区块链记录，用于记录对实体证书的操作记录；所述装置包括：

接收模块 1101，用于接收第一 CA 实体的证书共识请求；共识模块 1102，用于根据所述第一 CA 实体的证书共识请求，对所述第一 CA 实体的待签发实体证书进行共识，所述待签发实体证书中包括区块链认证标记，其中所述区块链认证标记为所述区块链系统的标识；更新模块 1103，用于若确定对所述待签发实体证书的认证通过，则更新存储的区块链记录。

具体的，所述更新模块 1103 具体用于，在所述区块链记录中，增加所述待签发实体证书对应的新增记录。

具体的，所述更新模块 1103 具体用于，当有实体证书更新时，在所述区块链记录中，增加对进行更新的实体证书对应的更新记录。

其中，所述接收模块 1101 还用于，接收所述第一 CA 实体的证书吊销请求，根据所述证书吊销请求确定是否通过所述证书吊销请求；所述更新模块 1103 具体用于，当通过所述证书吊销请求时，在所述区块链记录中，增加被吊销的实体证书对应的吊销记录。

本公开所述装置的工作原理可参照前述方法实施例的描述。

在本公开的一些实施例中，可实现基于区块链认证标记进行证书的相关处理，无需复杂的网状交叉认证，无需依靠公信力更高的权威中介建立桥接关系，即可实现每用户证书粒度的精细互信控制。因此，利用本公开的一些实施例的方案，提高了实现 CA 互信的灵活性。

本公开的一些实施例的电子设备包括处理器 1201 和存储器 1202，所述存储器 1202 用于存储计算机程序。其中，当所述处理器 1201 调用并且执行在所述存储器 1202 上存储的所述计算机程序时，所述处理器 1201 实现如前述任一实施例的实现 CA 互信的方法。

本公开的一些实施例的计算机可读存储介质，用于存储计算机程序，其中，所述计算机程序可被处理器执行如前述任一实施例的实现 CA 互信的方法。

在本申请所提供的几个实施例中，应该理解到，所揭露方法和装置，可以通过其它的方式实现。例如，以上所描述的装置实施例仅仅是示意性的，例如，所述单元的划分，仅仅为一种逻辑功能划分，实际实现时可以有另外的划分方式，例如多个单元或组件可以结合或者可以集成到另一个系统，或一些特征可以忽略，或不执行。另一点，所显示或讨论的相互之间的耦合或直接耦合或通信连接可以是通过一些接口，装置或单元的间接耦合或通信连接，可以是电性，机械或其它的形式。

另外，在本公开各个实施例中的各功能单元可以集成在一个处理单元中，也可以是各个单元单独物理包括，也可以两个或两个以上单元集成在一个单元中。上述集成的单元既可以采用硬件的形式实现，也可以采用硬件加软件功能单元的形式实现。

上述以软件功能单元的形式实现的集成的单元，可以存储在一个计算机可读取存储介质中。上述软件功能单元存储在一个存储介质中，包括若干指令用以使得一台计算机设备（可以是个人计算机，服务器，或者网络设备等）执行本公开各个实施例所述收发方法的部分步骤。而前述的存储介质包括：U 盘、移动硬盘、只读存储器（Read-Only Memory，简称 ROM）、易失性或非易失性随机存取存储器（Random Access Memory，简称 RAM）、磁碟或者光盘等各种可以存储程序代码的介质。

以上所述是本公开的可选实施方式，应当指出，对于本技术领域的普通技术人员来说，在不脱离本公开所述原理的前提下，还可以作出若干改进和润饰，这些改进和润饰也应视为本公开的保护范围。

权利要求书

1、一种实现证书权威 CA 互信的方法，该方法应用于 CA 互信系统中的 CA 实体，所述 CA 互信系统包括至少三个 CA 实体，各 CA 实体组成点到点 P2P 网络并形成区块链系统，各 CA 实体中存储有区块链记录，区块链记录用于记录对实体证书的操作记录，所述方法包括：

为证书请求方分配待签发实体证书；

向所述系统中的其他 CA 实体请求对所述待签发实体证书进行共识；

若确定所述其他 CA 实体对所述待签发实体证书的共识通过，则向所述证书请求方签发所述待签发实体证书，在所述待签发实体证书中包括区块链认证标记，其中所述区块链认证标记为所述区块链系统的标识；以及

更新存储的区块链记录。

2、根据权利要求 1 所述的方法，其中，所述各 CA 实体分别对应设置有互信代理，各 CA 实体通过对应设置的互信代理组成 P2P 网络并形成区块链系统，所述区块链记录存储在所述互信代理中。

3、根据权利要求 1 或 2 所述的方法，其中，所述为证书请求方分配待签发实体证书，包括：

接收所述证书请求方的证书申请请求；

根据所述证书申请请求对所述证书请求方进行身份鉴别，获得所述证书请求方的身份鉴别信息；以及

当对所述证书请求方的身份鉴别通过后，为所述证书请求方分配所述待签发实体证书。

4、根据权利要求 2 所述的方法，其中，所述向所述系统中的其他 CA 实体请求对所述待签发实体证书进行共识，包括：

通过对应设置的互信代理，向所述系统中其他 CA 实体对应的互信代理模块请求对所述待签发实体证书进行共识；

所述若确定所述其他 CA 实体对所述待签发实体证书的共识通过，则向所述证书请求方签发所述待签发实体证书，包括：

若确定所述其他 CA 实体对应的互信代理模块对所述待签发实体证书的

共识通过，则向所述证书请求方签发所述待签发实体证书；并且

所述更新存储的区块链记录，包括：

在所述区块链记录中，增加所述待签发实体证书对应的新增记录。

5、根据权利要求 4 所述的方法，其中，所述通过对应设置的互信代理，向所述系统中其他 CA 实体对应的互信代理模块请求对所述待签发实体证书进行共识，包括：

通过对应设置的互信代理，向所述系统中其他 CA 实体对应的互信代理模块发送所述待签发实体证书、所述证书请求方的身份鉴别信息，以请求对所述待签发实体证书进行共识。

6、根据权利要求 1 或 2 所述的方法，其中，所述 CA 互信系统还包括各 CA 实体对应的中间 CA 实体，

所述向所述证书请求方签发所述待签发实体证书，包括：

通过所述中间 CA 实体向所述证书请求方签发所述待签发实体证书。

7、根据权利要求 1 或 2 所述的方法，还包括：

若确定所述其他 CA 实体对所述待签发实体证书的共识未通过，则删除所述待签发实体证书，并向所述证书请求方签发最终实体证书，其中所述最终实体证书中不包括所述区块链认证标记。

8、根据权利要求 2 所述的方法，其中，在所述为证书请求方分配待签发实体证书的步骤之前，所述方法还包括：

接收所述证书请求方的证书更新请求；

所述为证书请求方分配待签发实体证书，包括：

根据所述证书更新请求，为所述证书请求方分配新的待签发实体证书；

所述向所述系统中的其他 CA 实体请求对所述待签发实体证书进行共识，包括：

通过对应设置的互信代理，向所述系统中的其他 CA 实体对应的互信代理请求对所述新的待签发实体证书进行共识；

所述若确定所述其他 CA 实体对所述待签发实体证书的共识通过，则向所述证书请求方签发所述待签发实体证书，包括：

所述若确定所述其他 CA 实体对应的互信代理对所述新的待签发实体证

书的共识通过，则向所述证书请求方签发所述新的待签发实体证书；并且
所述更新存储的区块链记录，包括：

在所述区块链记录中，增加所述证书请求方的原实体证书对应的更新记录。

9、根据权利要求 2 或 8 所述的方法，还包括：

通知所述其他 CA 实体吊销所述证书请求方的原实体证书。

10、根据权利要求 9 所述的方法，其中，所述通知所述其他 CA 实体吊销所述证书请求方的原实体证书，包括：

通过对应设置的互信代理，向所述其他 CA 实体对应的互信代理发送证书吊销请求，请求吊销所述证书请求方的原实体证书；并且

所述更新存储的区块链记录，包括：

在所述区块链记录中，增加所述原实体证书对应的吊销记录。

11、根据权利要求 2 所述的方法，还包括：

接收证书验证请求方的证书验证请求，在所述证书验证请求中包括待验证实体证书；

根据所述待验证实体证书确定根 CA 实体，并与所述根 CA 实体交互完成对所述待验证实体证书的验证，获得第一验证结果；

确定所述待验证实体证书中是否包含区块链认证标记；

若包含所述区块链认证标记，则利用对应设置的互信代理和所述区块链认证标记查找存储的区块链记录，根据查找确定是否通过对所述待验证实体证书的验证，获得第二验证结果；以及

根据所述第一验证结果和所述第二验证结果，向所述证书验证请求方发送最终的验证结果。

12、根据权利要求 11 所述的方法，其中，所述根据所述第一验证结果和所述第二验证结果，向所述证书验证请求方发送最终的验证结果，包括：

若所述第一验证结果和所述第二验证结果均表示通过对所述待验证实体证书的验证，则向所述证书验证请求方发送所述第一验证结果和/或所述第二验证结果；以及

若所述第一验证结果和所述第二验证结果不一致，则根据设置的验证结

果选择信息，选择优先级较高的验证结果作为最终的验证结果，并向所述证书验证请求方发送所述最终的验证结果。

13、一种实现证书权威 CA 互信的方法，该方法应用于 CA 互信系统中的 CA 实体，所述 CA 互信系统包括至少三个 CA 实体，各 CA 实体组成点对点 P2P 网络并形成区块链系统，各 CA 实体中存储有区块链记录，区块链记录用于记录对实体证书的操作记录，所述方法包括：

接收第一 CA 实体的证书共识请求；

根据所述第一 CA 实体的证书共识请求，对所述第一 CA 实体的待签发实体证书进行共识，所述待签发实体证书中包括区块链认证标记，其中所述区块链认证标记为所述区块链系统的标识；以及

若确定对所述待签发实体证书的共识通过，则更新存储的区块链记录。

14、根据权利要求 13 所述的方法，其中，所述更新存储的区块链记录，包括：

在所述区块链记录中，增加所述待签发实体证书对应的新增记录。

15、根据权利要求 14 所述的方法，其中，所述更新存储的区块链记录，还包括：

当有实体证书更新时，在所述区块链记录中，增加对进行更新的实体证书对应的更新记录。

16、根据权利要求 15 所述的方法，还包括：

接收所述第一 CA 实体的证书吊销请求，根据所述证书吊销请求确定是否通过所述证书吊销请求；并且

所述更新存储的区块链记录，包括：

当通过所述证书吊销请求时，在所述区块链记录中，增加被吊销的实体证书对应的吊销记录。

17、一种实现证书权威 CA 互信的装置，该装置应用于 CA 互信系统中的 CA 实体，所述 CA 互信系统包括至少三个 CA 实体，各 CA 实体组成点对点 P2P 网络并形成区块链系统，各 CA 实体中存储有区块链记录，区块链记录用于记录对实体证书的操作记录；所述装置包括：

分配模块，用于为证书请求方分配待签发实体证书；

请求模块，用于向所述系统中的其他 CA 实体请求对所述待签发实体证书进行共识；

签发模块，用于若确定所述其他 CA 实体对所述待签发实体证书的共识通过，则向所述证书请求方签发所述待签发实体证书，在所述待签发实体证书中包括区块链认证标记，其中所述区块链认证标记为所述区块链系统的标识；以及

更新模块，用于更新存储的区块链记录。

18、根据权利要求 17 所述的装置，还包括：

互信代理模块，用于将所述实现 CA 互信的装置与其他 CA 实体组成 P2P 网络并形成区块链系统；所述区块链记录存储在所述互信代理模块中。

19、根据权利要求 17 或 18 所述的装置，其中，所述分配模块包括：

接收子模块，用于接收所述证书请求方的证书申请请求；

身份鉴别子模块，用于根据所述证书申请请求对所述证书请求方进行身份鉴别，获得所述证书请求方的身份鉴别信息；以及

分配子模块，用于当对所述证书请求方的身份鉴别通过后，为所述证书请求方分配所述待签发实体证书。

20、根据权利要求 18 所述的装置，其中，所述请求模块具体用于，通过对应设置的互信代理模块，向所述系统中其他 CA 实体对应的互信代理模块请求对所述待签发实体证书进行共识；

所述签发模块具体用于，若确定所述其他 CA 实体对应的互信代理模块对所述待签发实体证书的共识通过，则向所述证书请求方签发所述待签发实体证书；并且

所述更新模块具体用于，在所述区块链记录中，增加所述待签发实体证书对应的新增记录。

21、根据权利要求 20 所述的装置，其中，所述请求模块具体用于，通过对应设置的互信代理模块，向所述系统中其他 CA 实体对应的互信代理模块发送所述待签发实体证书、所述证书请求方的身份鉴别信息，以请求对所述待签发实体证书进行共识。

22、根据权利要求 17 或 18 所述的装置，其中，所述 CA 互信系统还包

括各 CA 实体对应的中间 CA 实体；

所述签发模块具体用于通过所述中间 CA 实体向所述证书请求方签发所述待签发实体证书。

23、根据权利要求 17 或 18 所述的装置，还包括：

删除模块，用于若确定所述其他 CA 实体对所述待签发实体证书的共识未通过，则删除所述待签发实体证书，并向所述证书请求方签发最终实体证书，其中所述最终实体证书中不包括所述区块链认证标记。

24、根据权利要求 18 所述的装置，还包括：

第一接收模块，用于接收所述证书请求方的证书更新请求；

所述分配模块具体用于，根据所述证书更新请求，为所述证书请求方分配新的待签发实体证书；

所述请求模块具体用于，通过对应设置的互信代理模块，向所述系统中的其他 CA 实体对应的互信代理模块请求对所述新的待签发实体证书进行共识；

所述签发模块具体用于，若确定所述其他 CA 实体对应的互信代理模块对所述新的待签发实体证书的共识通过，则向所述证书请求方签发所述新的待签发实体证书；并且

所述更新模块具体用于，在所述区块链记录中，增加所述证书请求方的原实体证书对应的更新记录。

25、根据权利要求 18 或 24 所述的装置，还包括：

通知模块，用于通知所述其他 CA 实体吊销所述证书请求方的原实体证书。

26、根据权利要求 25 所述的装置，其中，所述通知模块具体用于，通过所述互信代理模块，向所述其他 CA 实体对应的互信代理模块发送证书吊销请求，请求吊销所述证书请求方的原实体证书；并且

所述更新模块具体用于，在所述区块链记录中，增加所述原实体证书对应的吊销记录。

27、根据权利要求 18 所述的装置，还包括：

第二接收模块，用于接收证书验证请求方的证书验证请求，在所述证书

验证请求中包括待验证实体证书；

第一验证模块，用于根据所述待验证实体证书确定根 CA 实体，并与所述根 CA 实体交互完成对所述待验证实体证书的验证，获得第一验证结果；

第一确定模块，用于确定所述待验证实体证书中是否包含区块链认证标记；

第二验证模块，用于若包含所述区块链认证标记，则利用对应设置的互信代理模块和所述区块链认证标记查找存储的区块链记录，根据查找确定是否通过对所述待验证实体证书的验证，获得第二验证结果；以及

结果发送模块，用于根据所述第一验证结果和所述第二验证结果，向所述证书验证请求方发送最终的验证结果。

28、根据权利要求 27 所述的装置，其中，所述结果发送模块具体用于，若所述第一验证结果和所述第二验证结果均表示通过对所述待验证实体证书的验证，则向所述证书验证请求方发送所述第一验证结果和/或所述第二验证结果；并且

若所述第一验证结果和所述第二验证结果不一致，则根据设置的验证结果选择信息，选择优先级较高的验证结果作为最终的验证结果，并向所述证书验证请求方发送所述最终的验证结果。

29、一种实现证书权威 CA 互信的装置，该装置应用于 CA 互信系统中的 CA 实体，所述 CA 互信系统包括至少三个 CA 实体，各 CA 实体组成点到点 P2P 网络并形成区块链系统，各 CA 实体中存储有区块链记录，区块链记录用于记录对实体证书的操作记录，所述装置包括：

接收模块，用于接收第一 CA 实体的证书共识请求；

共识模块，用于根据所述第一 CA 实体的证书共识请求，对所述第一 CA 实体的待签发实体证书进行共识，所述待签发实体证书中包括区块链认证标记，其中所述区块链认证标记为所述区块链系统的标识；以及

更新模块，用于若确定对所述待签发实体证书的共识通过，则更新存储的区块链记录。

30、根据权利要求 29 所述的装置，其中，所述更新模块具体用于，在所述区块链记录中，增加所述待签发实体证书对应的新增记录。

31、根据权利要求 30 所述的装置，其中，所述更新模块具体用于，当有实体证书更新时，在所述区块链记录中，增加对进行更新的实体证书对应的更新记录。

32、根据权利要求 31 所述的装置，其中，所述接收模块还用于，接收所述第一 CA 实体的证书吊销请求，根据所述证书吊销请求确定是否通过所述证书吊销请求；以及

所述更新模块具体用于，当通过所述证书吊销请求时，在所述区块链记录中，增加被吊销的实体证书对应的吊销记录。

33、一种实现证书权威 CA 互信的系统，包括：

至少三个 CA 实体，各 CA 实体组成点到点 P2P 网络并形成区块链系统；
各 CA 实体中存储有区块链记录，用于记录对实体证书的操作记录；

其中，所述至少三个 CA 实体中的第一 CA 实体，为证书请求方分配待签发实体证书，并向所述系统中的第二 CA 实体请求对所述待签发实体证书进行共识；若确定所述第二 CA 实体对所述待签发实体证书的共识通过，则向所述证书请求方签发所述待签发实体证书，在所述待签发实体证书中包括区块链认证标记，其中所述区块链认证标记为所述区块链系统的标识，并更新存储的区块链记录；

所述至少三个 CA 实体中的第二 CA 实体，接收所述第一 CA 实体的证书共识请求，并根据所述第一 CA 实体的证书共识请求，对所述第一 CA 实体的待签发实体证书进行共识，若确定对所述待签发实体证书的共识通过，则更新存储的区块链记录。

34、根据权利要求 33 所述的系统，其中，所述各 CA 实体分别对应设置有互信代理，各 CA 实体通过对应设置的互信代理组成 P2P 网络并形成区块链系统；所述区块链记录存储在所述互信代理中。

35、一种电子设备，包括：

处理器，

存储器，用于存储计算机程序；

其中，所述处理器在调用并执行所述存储器上存储的计算机程序时，所述处理器实现如权利要求 1-12 任一项所述的实现证书权威 CA 互信的方法。

36、一种计算机可读存储介质，包括：

在所述计算机可读存储介质上存储的计算机程序，

其中，当所述计算机程序被处理器执行时，所述处理器执行如权利要求 1-12 任一项所述的实现证书权威 CA 互信的方法。

37、一种电子设备，包括：

处理器，

存储器，用于存储计算机程序；

其中，所述处理器在调用并执行所述存储器上存储的计算机程序时，所述处理器实现如权利要求 13-16 任一项所述的实现证书权威 CA 互信的方法。

38、一种计算机可读存储介质，包括：

在所述计算机可读存储介质上存储的计算机程序，

其中，当所述计算机程序被处理器执行时，所述处理器执行如权利要求 13-16 任一项所述的实现证书权威 CA 互信的方法。

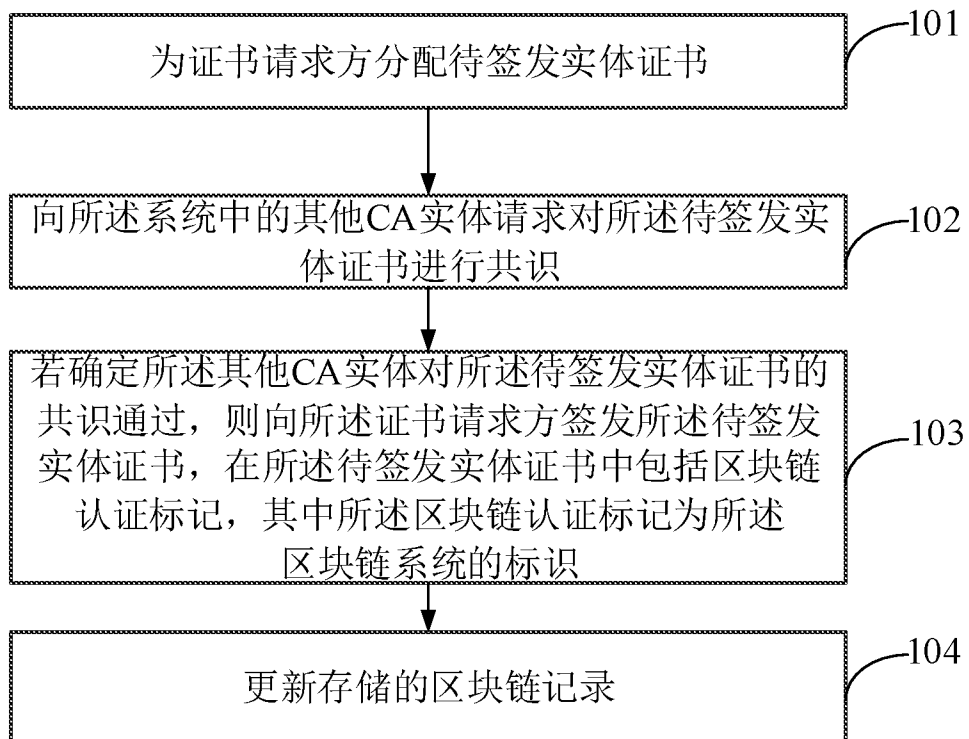


图 1

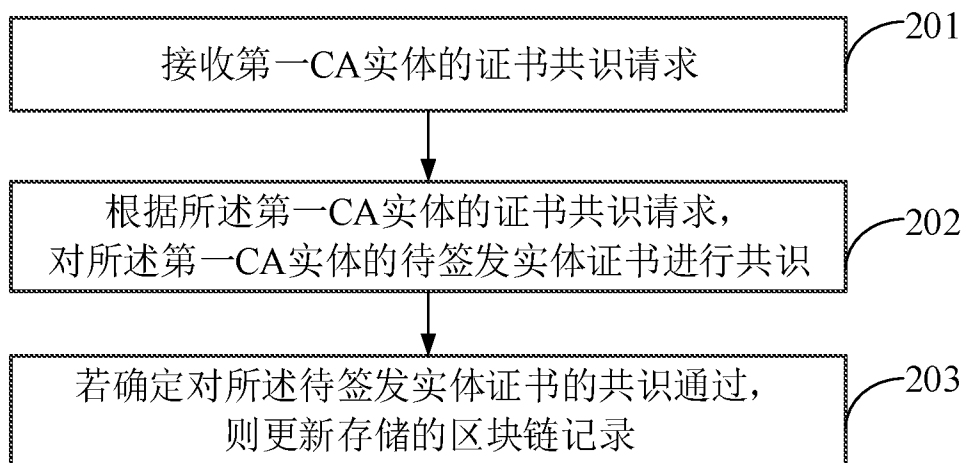


图 2

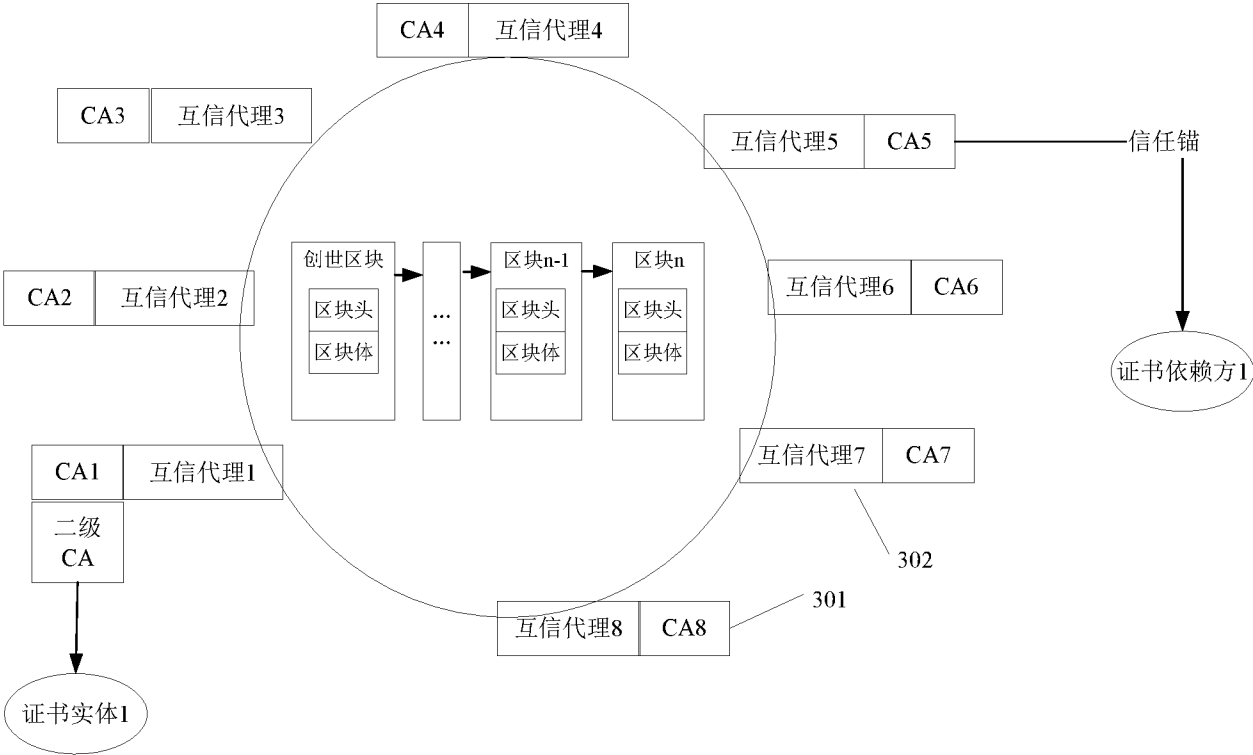


图 3

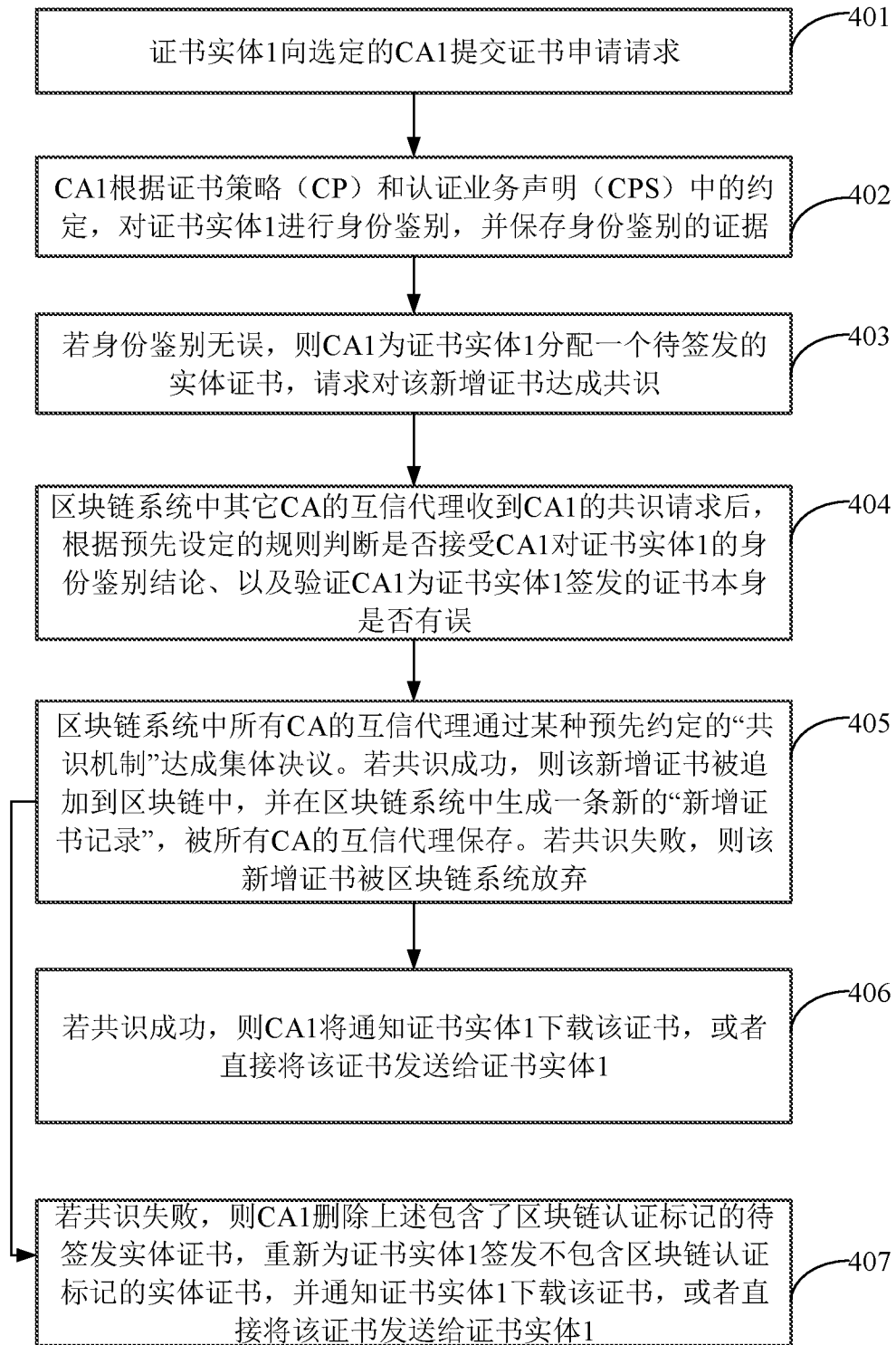


图 4

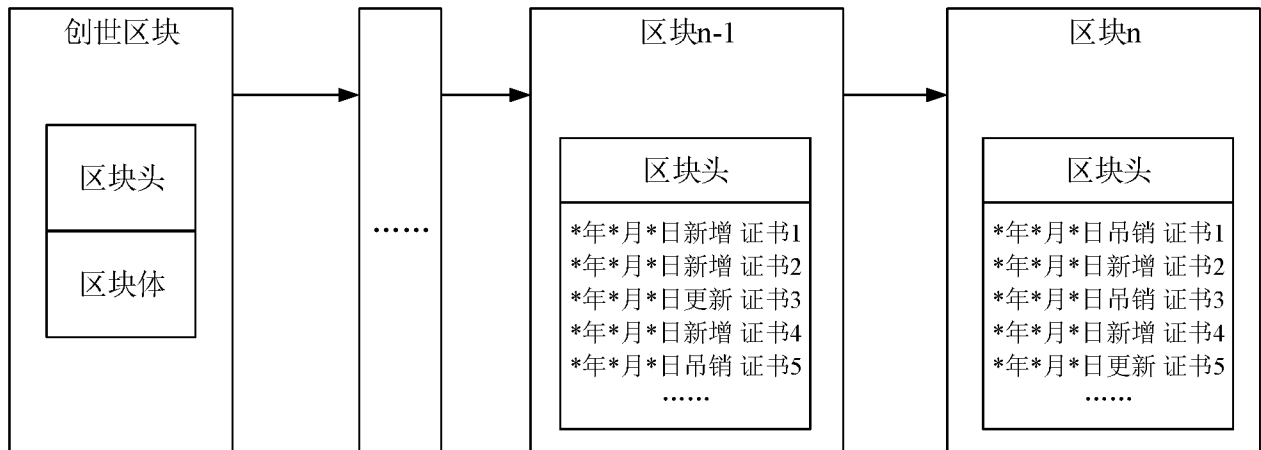


图 5

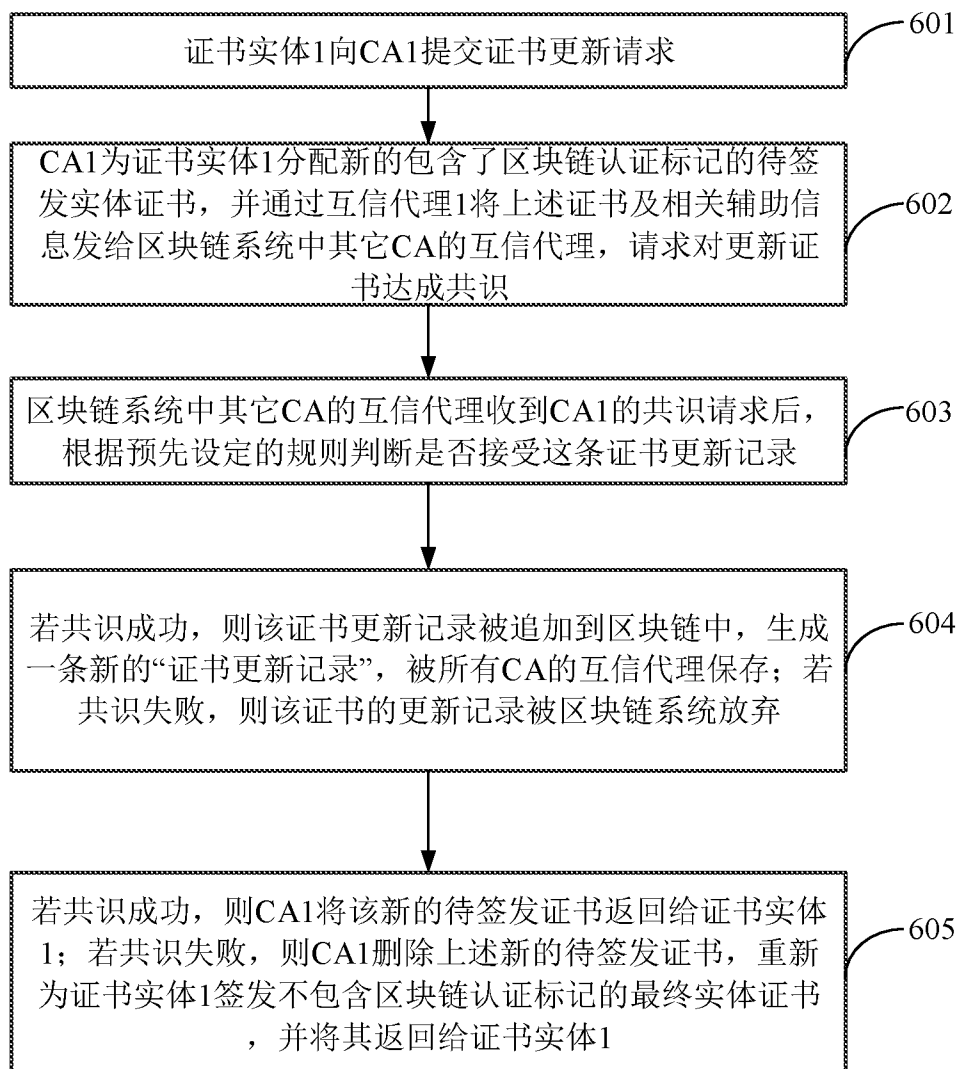


图 6

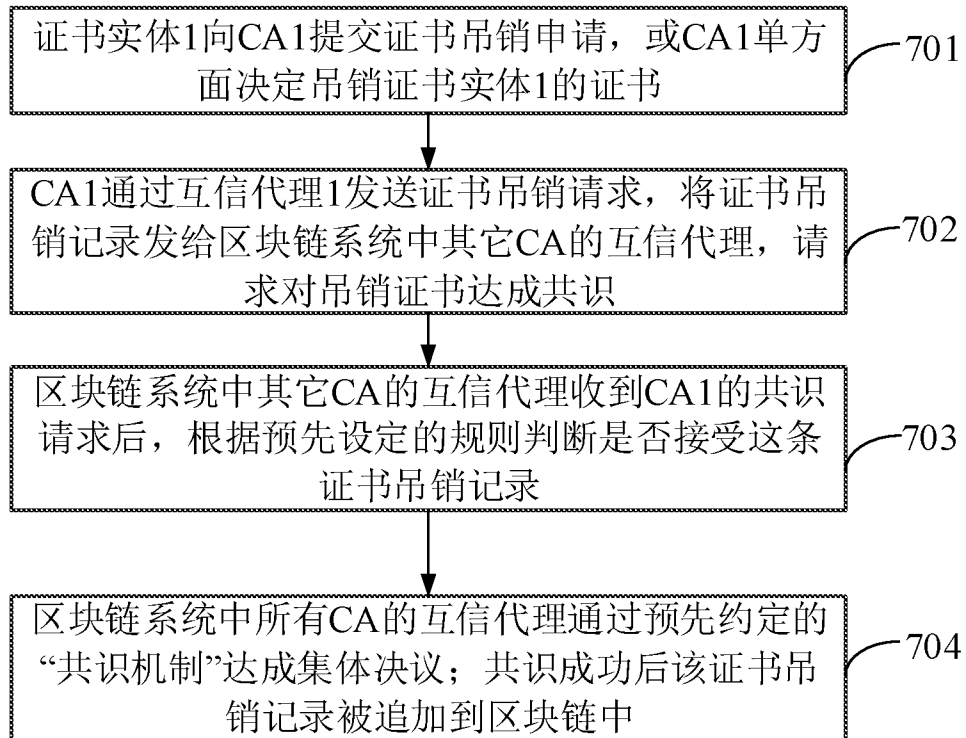


图 7

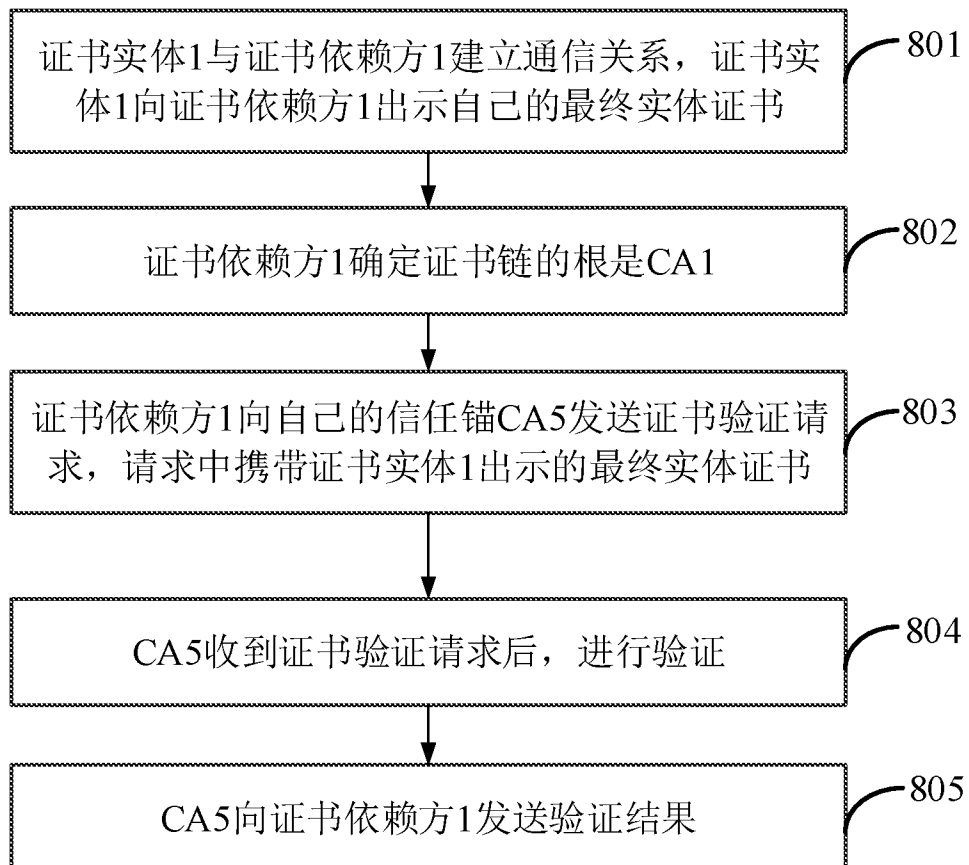


图 8

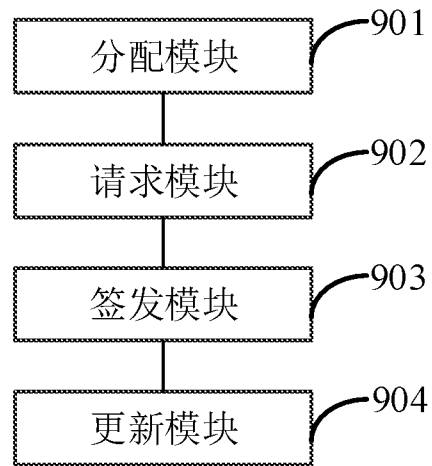


图 9

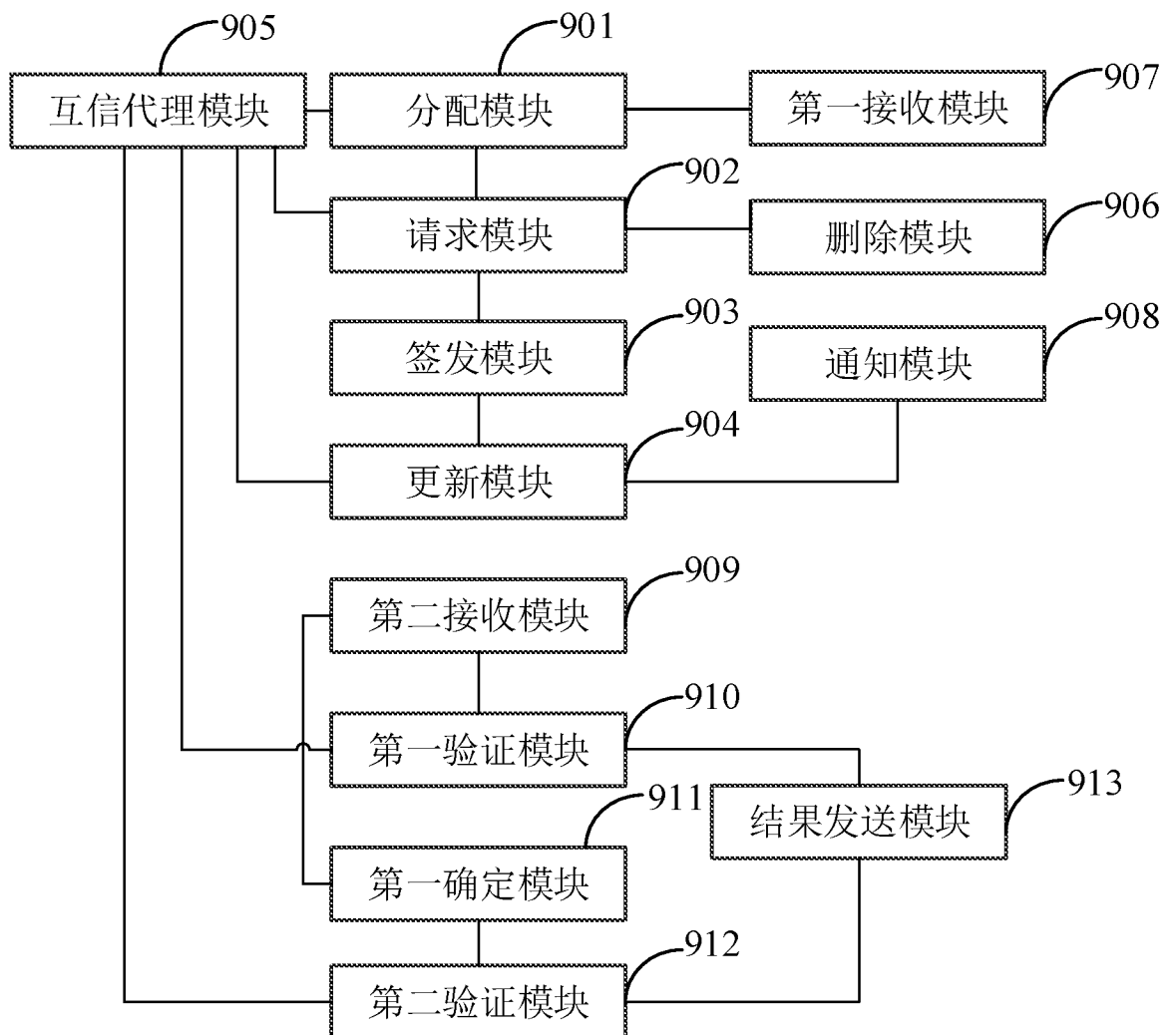


图 10

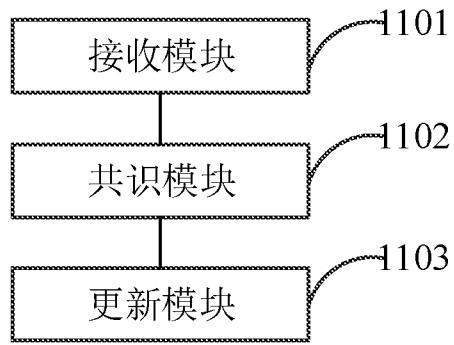


图 11

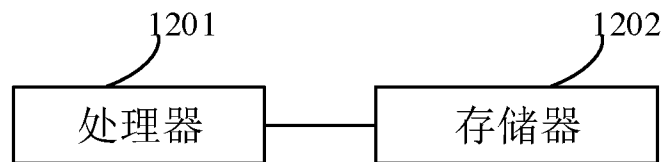


图 12

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2018/078848

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32 (2006.01) i; H04L 29/06 (2006.01) i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

CNXTX; CNABS; USTXT; EPTXT; WOTXT; VEN; CNKI: 证书权威, 证书, 授权, 互信, 信任, 点到点, 区块链, 共识, CA, P2P, certificate, authority, mutual, trust, blockchain, agreement

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 106301792 A (JIANGSU PAY EGIS TECHNOLOGY CO., LTD.) 04 January 2017 (04.01.2017), entire document	1-38
A	CN 105591753 A (HANGZHOU FUZAMEI TECHNOLOGY CO., LTD.) 18 May 2016 (18.05.2016), entire document	1-38
A	CN 106384236 A (JIANGSU PAY EGIS TECHNOLOGY CO., LTD.) 08 February 2017 (08.02.2017), entire document	1-38
A	WO 2017022917 A1 (COINPLUG INC.) 09 February 2017 (09.02.2017), entire document	1-38

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:

“A” document defining the general state of the art which is not considered to be of particular relevance

“E” earlier application or patent but published on or after the international filing date

“L” document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

“O” document referring to an oral disclosure, use, exhibition or other means

“P” document published prior to the international filing date but later than the priority date claimed

“T” later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

“X” document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

“Y” document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

“&” document member of the same patent family

Date of the actual completion of the international search
28 May 2018

Date of mailing of the international search report
08 June 2018

Name and mailing address of the ISA
State Intellectual Property Office of the P. R. China
No. 6, Xitucheng Road, Jimenqiao
Haidian District, Beijing 100088, China
Facsimile No. (86-10) 62019451

Authorized officer
ZOU, Ting
Telephone No. (86-10) 62089393

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2018/078848

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 106301792 A	04 January 2017	None	
CN 105591753 A	18 May 2016	None	
CN 106384236 A	08 February 2017	None	
WO 2017022917 A1	09 February 2017	KR 101661930 B1	05 October 2016

国际检索报告

国际申请号

PCT/CN2018/078848

A. 主题的分类 H04L 9/32 (2006.01) i; H04L 29/06 (2006.01) i 按照国际专利分类 (IPC) 或者同时按照国家分类和 IPC 两种分类																	
B. 检索领域 检索的最低限度文献 (标明分类系统和分类号) H04L 包含在检索领域中的除最低限度文献以外的检索文献 在国际检索时查阅的电子数据库 (数据库的名称, 和使用的检索词 (如使用)) CNTXT; CNABS; USTXT; EPTXT; WOTXT; VEN; CNKI: 证书权威, 证书, 授权, 互信, 信任, 点到点, 区块链, 共识, CA, P2P, certificate, authority, mutual, trust, blockchain, agreement																	
C. 相关文件 <table border="1"> <thead> <tr> <th>类 型*</th> <th>引用文件, 必要时, 指明相关段落</th> <th>相关的权利要求</th> </tr> </thead> <tbody> <tr> <td>A</td> <td>CN 106301792 A (江苏通付盾科技有限公司) 2017年 1月 4日 (2017 - 01 - 04) 全文</td> <td>1-38</td> </tr> <tr> <td>A</td> <td>CN 105591753 A (杭州复杂美科技有限公司) 2016年 5月 18日 (2016 - 05 - 18) 全文</td> <td>1-38</td> </tr> <tr> <td>A</td> <td>CN 106384236 A (江苏通付盾科技有限公司) 2017年 2月 8日 (2017 - 02 - 08) 全文</td> <td>1-38</td> </tr> <tr> <td>A</td> <td>WO 2017022917 A1 (COINPLUG INC) 2017年 2月 9日 (2017 - 02 - 09) 全文</td> <td>1-38</td> </tr> </tbody> </table>			类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求	A	CN 106301792 A (江苏通付盾科技有限公司) 2017年 1月 4日 (2017 - 01 - 04) 全文	1-38	A	CN 105591753 A (杭州复杂美科技有限公司) 2016年 5月 18日 (2016 - 05 - 18) 全文	1-38	A	CN 106384236 A (江苏通付盾科技有限公司) 2017年 2月 8日 (2017 - 02 - 08) 全文	1-38	A	WO 2017022917 A1 (COINPLUG INC) 2017年 2月 9日 (2017 - 02 - 09) 全文	1-38
类 型*	引用文件, 必要时, 指明相关段落	相关的权利要求															
A	CN 106301792 A (江苏通付盾科技有限公司) 2017年 1月 4日 (2017 - 01 - 04) 全文	1-38															
A	CN 105591753 A (杭州复杂美科技有限公司) 2016年 5月 18日 (2016 - 05 - 18) 全文	1-38															
A	CN 106384236 A (江苏通付盾科技有限公司) 2017年 2月 8日 (2017 - 02 - 08) 全文	1-38															
A	WO 2017022917 A1 (COINPLUG INC) 2017年 2月 9日 (2017 - 02 - 09) 全文	1-38															
☐ 其余文件在C栏的续页中列出。 ☒ 见同族专利附件。																	
* 引用文件的具体类型: “A” 认为不特别相关的表示了现有技术一般状态的文件 “E” 在国际申请日的当天或之后公布的在先申请或专利 “L” 可能对优先权要求构成怀疑的文件, 或为确定另一篇引用文件的公布日而引用的或者因其他特殊理由而引用的文件 (如具体说明的) “O” 涉及口头公开、使用、展览或其他方式公开的文件 “P” 公布日先于国际申请日但迟于所要求的优先权日的文件 “T” 在申请日或优先权日之后公布, 与申请不相抵触, 但为了理解发明之理论或原理的在后文件 “X” 特别相关的文件, 单独考虑该文件, 认定要求保护的发明不是新颖的或不具有创造性 “Y” 特别相关的文件, 当该文件与另一篇或者多篇该类文件结合并且这种结合对于本领域技术人员为显而易见时, 要求保护的发明不具有创造性 “&” 同族专利的文件																	
国际检索实际完成的日期 2018年 5月 28日		国际检索报告邮寄日期 2018年 6月 8日															
ISA/CN的名称和邮寄地址 中华人民共和国国家知识产权局 (ISA/CN) 中国北京市海淀区蓟门桥西土城路6号 100088 传真号 (86-10) 62019451		授权官员 邹婷 电话号码 86- (010) -62089393															

国际检索报告
关于同族专利的信息

国际申请号

PCT/CN2018/078848

检索报告引用的专利文件			公布日 (年/月/日)	同族专利	公布日 (年/月/日)
CN	106301792	A	2017年 1月 4日	无	
CN	105591753	A	2016年 5月 18日	无	
CN	106384236	A	2017年 2月 8日	无	
WO	2017022917	A1	2017年 2月 9日	KR 101661930 B1	2016年 10月 5日