(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 106936566 B
(45)授权公告日 2020.03.31

(21)申请号 201710139573.6

(22)申请日 2017.03.09

(65)同一申请的已公布的文献号
申请公布号 CN 106936566 A

(43)申请公布日 2017.07.07

(73)专利权人 江苏省南京市南京公证处
地址 210005 江苏省南京市长江路99号长江贸易大楼7层
专利权人 江苏慧世联网络科技有限公司

(72)发明人 陈宁娟 葛峰 韩金广

(74)专利代理机构 北京思创大成知识产权代理有限公司 11614
代理人 王尧

(51)Int.Cl.
*H04L 9/00*(2006.01)
*H04L 9/06*(2006.01)
*H04L 9/08*(2006.01)
*G06Q 50/18*(2012.01)

(56)对比文件
CN 106301792 A,2017.01.04,全文.
CN 105701372 A,2016.06.22,全文.
CN 105635169 A,2016.06.01,全文.

审查员 孙方涛

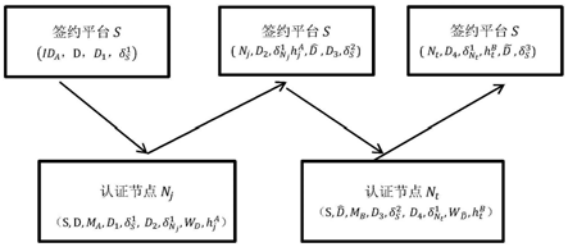
权利要求书4页 说明书8页 附图1页

(54)发明名称

一种基于区块链技术的可外包的文书签署方法

(57)摘要

一种基于区块链技术的可外包的文书签署方法，采用签约平台和区块链认证节点，该方法包括以下步骤：系统初始化步骤；秘钥管理系统初始化的步骤；用户注册的步骤；用户发起签约的步骤。本发明基于区块链技术、外包计算和文书签署技术而提出，相对于传统的文书签署方法，用户不需要保存文书及签名；文书签署过程被详细记录，并且不能被篡改；用户可以将签署运算外包给签约平台完成；多个区块链公证节点的存在可以抵抗签约平台与公证平台的合谋攻击。




CN 106936566 B

1.一种基于区块链技术的可外包的文书签署方法，采用签约平台和区块链认证节点，其特征是该方法包括以下步骤：

S1、系统初始化步骤：

S1-1、根据安全级别，为签约平台S和区块链认证节点$N_i$选择安全参数γ，i＝1,2,…,n，i表示区块链认证节点的编号，n表示区块链认证节点的总数；

S1-2、为签约平台S和区块链认证节点$N_i$选择哈希函数H，加密、解密算法(Enc,Dec)；签名、验证算法(Sign,Ver)和密钥产生算法KG；

S2、秘钥管理系统初始化的步骤：

S2-1、签约平台S输入安全参数γ，利用密钥产生算法产生S的私钥$SK_S$和公钥$PK_S$，$KG(\gamma)\rightarrow(SK_S,PK_S)$；

S2-2、各认证节点$N_i$分别输入安全参数γ，利用密钥产生算法产生各自的私钥$SK_{N_i}$和公钥$PK_{N_i}$，$KG(\gamma)\rightarrow(SK_{N_i},PK_{N_i})$；

S2-3、签约平台S与认证节点$N_i$利用现有密钥交换技术交换密钥$K_i$，签约平台保存信息$(N_i,K_i)$，认证平台$N_i$保存信息$K_i$；

S3、用户注册的步骤：

各用户X向签约平台S提交注册信息$ID_X$，并且设置登录密码$P_X$，注册信息$ID_X$包括身份证件号码$IDN_X$、手机号码$M_X$以及用户名$U_X$；

S4、用户发起签约的步骤：

S4-1、Alice登录签约平台S，将文书D导入到签约平台，选择与用户Bob签约；

S4-2、签约平台S对文书D进行下述计算，得到摘要$D_1$，签名$\delta_S^1$以及加密文书$C_S^1$；

$D_1=H(D)$，

$$\delta_S^1=sign(SK_S,\ D_1),$$

$$C_S^1=Enc(r_s^1,D);$$

其中，$r_S^1$表示签约平台的随机参数；

签约平台S利用区块链技术保存$(ID_A,D,D_1,\ \delta_S^1)$，并且将$(M_A,\ C_S^1)$广播给所有认证节点请求认证节点对该签约任务进行认证和提供认证签约码；

S4-3、认证节点$N_j$，j∈{1,2,…,n}随机响应签约平台的请求，接受对签约任务进行认证服务，并就此通知签约平台；

S4-4、签约平台S加密随机参数$r_S^1$和签名$\delta_S^1$，得到密文$C_{S,N_j,1}=Enc(K_j,\ r_S^1)$，和$C_{S,N_j,2}=Enc(K_j,\ \delta_S^1)$，将$C_{S,N_j,1}$、$C_{S,N_j,2}$、$C_S^1$发送给响应的认证节点$N_j$；

S4-5、认证节点$N_j$利用密钥$K_j$解密$C_{S,N_j,1}$、$C_{S,N_j,2}$，获得$r_S^1=Dec(K_j,C_{S,N_j,1})$，$\delta_S^1=Dec(K_j,C_{S,N_j,2})$；$N_j$利用$r_S^1$解密$C_S^1$，获得$D=Dec(r_S^1,\ C_S^1)$；$N_j$将文书D存放在随机存储位置$W_D$；

认证平台$N_j$进行下述计算，获取摘要$D_1$、$D_2$、签名$\delta_{N_j}^1$、签约码$h_j^A$；

$D_1=H(D)$，

$D_2=H(D_1||W_D)$，

$$\delta_{N_j}^1 = sign(SK_{N_j}, D_2),$$

$$h_j^A = H(K_j||r_j^A);$$

其中，$r_j^A$为认证节点$N_j$选择的随机参数，认证节点将$(W_D, r_j^A)$通过短信发送给Alice，将$(D_2, \delta_{N_j}^1, h_j^A)$发送给签约平台S；认证节点$N_j$利用区块链技术保存$(S, D, M_A, D_1, \delta_S^1, D_2, \delta_{N_j}^1, W_D, h_j^A)$，S表示签约平台的名称；

S4-6、签约平台通知Alice确认签约文书；

S4-7、Alice利用访问位置$W_D$查看文书D，Alice比对D是否与原文一致，如果一致，执行S4-8；否则，签约失败；

S4-8、Alice决定是否签署文书，如果决定签署，执行S4-9；否则，签约终止；

S4-9、Alice在签约平台S输入$r_j^A$；

S4-10、签约平台S根据Alice输入的随机参数$r_j^A$计算签约码$h_j^{A\prime} = H(K_j||r_j^A)$，判断签约平台计算的签约码与认证节点发送的签约码是否一致，如果$h_j^{A\prime} = h_j^A$等式成立，执行S4-11，否则签署失败；

S4-11、签约平台S利用Alice身份对文书D进行签名，得到文书$\widehat{D}$，签约平台S进行下述计算，获取摘要$D_3$，签名$\delta_S^2$以及加密文书$C_S^2$；

$$D_3 = H\left(D_2||\widehat{D}\right),$$

$$\delta_S^2 = sign(SK_S, D_3),$$

$$C_S^2 = Enc(r_s^2, \widehat{D});$$

其中，$r_S^2$表示签约平台的随机参数；

签约平台S利用区块链技术保存$(N_j, D_2, \delta_{N_j}^1 h_j^A, \widehat{D}, D_3, \delta_S^2)$，将$(M_B, C_S^2)$广播给所有认证节点，请求认证节点对签约任务进行认证和提供签约码；同时签约平台S通知用户Bob登录签约平台S查看文书$\widehat{D}$的签署任务；

S4-12、认证节点$N_t$，$t\in\{1,2,\cdots,n\}$随机响应签约平台的请求，决定为对该签约任务提供认证服务；

S4-13、签约平台S加密随机参数$r_S^2$和签名$\delta_S^2$，得到密文$C_{S,N_t,1} = Enc(K_t,\ r_S^2)$，$C_{S,N_t,2} = Enc(K_t,\ \delta_S^2)$，并将$C_{S,N_t,1}$、$C_{S,N_t,2}$和$C_S^2$发送给响应的认

证节点$N_t$；

S4-14、认证节点$N_t$利用密钥$N_t$解密$C_{S,N_t,1}$和$C_{S,N_t,2}$，获得$r_S^2 = Dec(K_t, C_{S,N_t,1})$，$\delta_S^2 = Dec(K_t, C_{S,N_t,2})$；$N_t$利用$r_S^2$解密$C_S^2$，获得$\widehat{D} = Dec(r_S^2, C_S^2)$；$N_t$将文书$\widehat{D}$存放在随机存储位置$W_{\widehat{D}}$；

认证平台$N_t$进行下述计算，获取摘要$D_4$、签名$\delta_{N_t}^1$、签约码$h_t^A$；

$$D_4 = H(D_3||W_{\widehat{D}}),$$

$$\delta_{N_t}^1 = sign(SK_{N_t}, D_4),$$

$$h_t^B = H(K_t||r_t^B);$$

其中，$r_t^B$为认证节点$N_t$选择的随机参数，认证节点将$(W_{\widehat{D}}, r_t^B)$通过短信发送给Bob，将$(D_4, \delta_{N_t}^1, h_t^B)$发送给签约平台S，认证节点$N_t$利用区块链技术保存$(S, \widehat{D}, M_B, D_3, \delta_S^2, D_4, \delta_{N_t}^1, W_{\widehat{D}}, h_t^B)$；

S4-15、签约平台通知Bob确认签约文书；

S4-16、Bob利用访问$W_{\widehat{D}}$查看文书$\widehat{D}$，Bob比对$\widehat{D}$是否与签约平台展示的文书内容一致，如果一致，执行S4-17；否则，签约失败；

S4-17、Bob在签约平台S输入$r_t^B$；

S4-18、签约平台S根据Bob输入的随机参数$r_t^B$计算签约码$h_t^{B\prime} = H(K_t||r_t^B)$，判断签约平台计算的签约码与认证节点发送的签约码是否一致，如果$h_t^{B\prime} = h_t^B$等式成立，执行S4-19，否则签署失败；

S4-19、签约平台S利用Bob身份对文书$\widehat{D}$进行签名，得到文书$\widetilde{D}$，签约平台S进行下述计算，获取摘要$D_5$以及签名$\delta_S^3$；

$$D_5 = H(D_4||\widetilde{D}),$$

$$\delta_S^3 = sign(SK_S, D_5),$$

S利用区块链技术保存$(N_t, D_4, \delta_{N_t}^1, h_t^B, \widetilde{D}, \delta_S^3)$，完成签约。

2.根据权利要求1所述的基于区块链技术的可外包的文书签署方法，其特征是：步骤S3中，签约平台S验证用户注册信息的正确性，对其进行线上或者线下的身份审核。

3.根据权利要求1所述的基于区块链技术的可外包的文书签署方法，其特征是：步骤S4-5和S4-14中，随机存储位置$W_D$和$W_{\widehat{D}}$在对应的认证节点$N_j$和$N_t$上，或者在任何一个或者相应的两个存储平台P上。

4.根据权利要求1所述的基于区块链技术的可外包的文书签署方法，其特征是：各认证节点为各公证处提供的公证存储模块，或者第三方公证存储模块。

5.根据权利要求1所述的基于区块链技术的可外包的文书签署方法，其特征是：步骤S2-3中，密钥共享技术采用Diffie-Hellman密钥交换方法。

6.根据权利要求1所述的基于区块链技术的可外包的文书签署方法，其特征是：步骤S4-1中，Alice利用用户名$U_A$和密码$P_A$登录签约平台S。

7.根据权利要求1所述的基于区块链技术的可外包的文书签署方法，其特征是：步骤S4-4中，签约平台S广播$C_{S,N_j,1}$、$C_{S,N_j,2}$、$C_S^1$给所有的认证节点，对应的步骤4-5中，认证节点$N_j$解密$C_S^1$，获得文书D。

8.根据权利要求1所述的基于区块链技术的可外包的文书签署方法，其特征是：步骤S4-13中，签约平台S广播$C_{S,N_t,1}$、$C_{S,N_t,2}$和$C_S^2$给所有的认证节点，对应的步骤S4-14中，认证节点$N_t$解密$C_S^2$，获得文书$\widehat{D}$。

# 一种基于区块链技术的可外包的文书签署方法

## 技术领域

[0001] 本发明涉及文书签署领域，尤其是一种基于认证区块链的可外包的文书签署方法。

## 背景技术

[0002] 区块链是一个分布的数据存储方式。区块链存储了一个按序排列的记录名单，叫做块。每一个块都包含一个时戳以及与前一个块的连接。区块链是一个公开、分布的记账系统，用可验证和永久保存的方法记录通信双方/多方之间的通信过程。特别地，区块链可以防止数据被篡改。作为一个新的数据存储技术，区块链已被广泛关注。

[0003] 外包计算可以使一个计算能力有限的用户将大量、复杂的运算外包给具有较强能力的平台来完成，从而降低用户端的计算负担和存储成本。

[0004] 随着电子商务的发展，传统的纸质文书正在被电子文书所取代。但现有的电子文书的签署方法都是基于公钥基础设施/认证中心(PKI/CA)模式。在该模式中，用户与其公钥之间被用一个公钥证书来关联。公钥证书有效地解决了用户公钥的真实性和有效性问题。尽管如此，公钥证书的颁发依赖于认证中心，并且公钥证书库的管理和维护成本较高。证书获取和更新流程非常复杂，影响其使用的范围。现有的电子文书的签署方法存在以下问题：(1)用户需要具有一定的存储空间来存储签约文书及签名；(2)用户必须具有一定的计算能力；(3)不能记录签署的过程，即无法反映文书签署的发起方。然而，在实际应用中，用户的设施(手机)只具有较弱的计算能力和有限的存储空间。涉及到法律问题，需要明确签署的发起方信息。

[0005] 本发明将区块链技术、外包计算技术与文书签署技术相结合，提出的一种基于认证区块链的可外包的文书签署方法。

## 发明内容

[0006] 本发明的目的是针对上述问题，提出基于公证区块链的可外包的文书签署方法。

[0007] 本发明的技术方案是：

[0008] 一种基于区块链技术的可外包的文书签署方法，采用签约平台和区块链认证节点，该方法包括以下步骤：

[0009] S1、系统初始化步骤：

[0010] S1-1、根据安全级别，为签约平台S和区块链认证节点$N_i$选择安全参数$\gamma$，i＝1，2，…，n，i表示区块链认证节点的编号，n表示区块链认证节点的总数；

[0011] S1-2、为签约平台S和区块链认证节点$N_i$选择哈希函数H，加密、解密算法(Enc，Dec)；签名、验证算法(Sign，Ver)和密钥产生算法KG；

[0012] S2、秘钥管理系统初始化的步骤：

[0013] S2-1、签约平台S输入安全参数$\gamma$，利用密钥产生算法产生S的私钥$SK_S$和公钥$PK_S$，$KG(\gamma)\rightarrow(SK_S,PK_S)$；

[0014] S2-2、各认证节点$N_i$分别输入安全参数$\gamma$，利用密钥产生算法产生各自的私钥$SK_{N_i}$和公钥$PK_{N_i}$，$KG(\gamma) \rightarrow (SK_{N_i}, PK_{N_i})$；

[0015] S2-3、签约平台S与认证节点$N_i$利用现有密钥交换技术交换密钥$K_i$，签约平台保存信息$(N_i, K_i)$，认证平台$N_i$保存信息$K_i$；

[0016] S3、用户注册的步骤：

[0017] 各用户X向签约平台S提交注册信息$ID_X$，并且设置登录密码$P_X$，注册信息$ID_X$包括身份证件号码$IDN_X$、手机号码$M_X$以及用户名$U_X$；

[0018] S4、用户发起签约的步骤：

[0019] S4-1、Alice登录签约平台S，将文书D导入到签约平台，选择与用户Bob签约；

[0020] S4-2、签约平台S对文书D进行下述计算，得到摘要$D_1$，签名$\delta_S^1$以及加密文书$C_S^1$；

[0021] $D_1 = H(D)$，

[0022] $$\delta_S^1 = sign(SK_S, D_1),$$

[0023] $$C_S^1 = Enc(r_s^1, D);$$

[0024] 其中，$r_S^1$表示签约平台的随机参数；

[0025] 签约平台S利用区块链技术保存$(ID_A, D, D_1, \delta_S^1)$，并且将$(M_A, C_S^1)$广播给所有认证节点请求认证节点对该任务进行认证和提供认证签约码；

[0026] S4-3、认证节点$N_j$，$j \in \{1,2,\cdots,n\}$随机响应签约平台的请求，接受对该签约任务进行认证服务，并就此通知签约平台；

[0027] S4-4、签约平台S加密随机参数$r_S^1$和签名$\delta_S^1$，得到密文$C_{S,N_j,1} = Enc(K_j, r_S^1)$，和$C_{S,N_j,2} = Enc(K_j, \delta_S^1)$，将$C_{S,N_j,1}$、$C_{S,N_j,2}$、$C_S^1$发送给响应的认证节点$N_j$；

[0028] S4-5、认证节点$N_j$利用密钥$K_j$解密$C_{S,N_j,1}$、$C_{S,N_j,2}$，获得$r_S^1 = Dec(K_j, C_{S,N_j,1})$，$\delta_S^1 = Dec(K_j, C_{S,N_j,2})$；$N_j$利用$r_S^1$解密$C_S^1$，获得$D = Dec(r_S^1, C_S^1)$；$N_j$将文书D存放在随机存储位置$W_D$；

[0029] 认证平台$N_j$进行下述计算，获取摘要$D_1$、$D_2$、签名$\delta_{N_j}^1$、签约码$h_j^A$；

[0030] $D_1 = H(D)$，

[0031] $D_2 = H(D_1||W_D)$，

[0032] $$\delta_{N_j}^1 = sign(SK_{N_j}, D_2),$$

[0033] $$h_j^A = H(K_j||r_j^A);$$

[0034] 其中，$r_j^A$为认证节点$N_j$选择的随机参数，认证节点将$(W_D, r_j^A)$通过短信发送给Alice，将$(D_2, \delta_{N_j}^1, h_j^A)$发送给签约平台S；认证节点$N_j$利用区块链技术保存

$(S, D, M_A, D_1, \delta_S^1, D_2, \delta_{N_j}^1, W_D, h_j^A)$，S表示签约平台的名称；

[0035] S4-6、签约平台通知Alice确认签约文书；

[0036] S4-7、Alice利用访问位置$W_D$查看文书D，Alice比对D是否与原文一致，如果一致，执行S4-8；否则，签约失败；

[0037] S4-8、Alice决定是否签署文书，如果决定签署，执行S4-9；否则，签约终止；

[0038] S4-9、Alice在签约平台S输入$r_j^A$；

[0039] S4-10、签约平台S根据Alice输入的随机参数$r_j^A$计算签约码$h_j^{A\prime} = H(K_j||r_j^A)$，判断签约平台计算的签约码与认证节点发送的签约码是否一致，如果$h_j^{A\prime} = h_j^A$等式成立，执行S4-11，否则签署失败；

[0040] S4-11、签约平台S利用Alice身份对文书D进行签名，得到文书$\widehat{D}$，签约平台S进行下述计算，获取摘要$D_3$，签名$\delta_S^2$以及加密文书$C_S^2$；

[0041] $$D_3 = H\left(D_2||\widehat{D}\right),$$

[0042] $$\delta_S^2 = sign(SK_S, D_3),$$

[0043] $$C_S^2 = Enc(r_s^2, \widehat{D});$$

[0044] 其中，$r_S^2$表示签约平台的随机参数；

[0045] 签约平台S利用区块链技术保存$(N_j, D_2, \delta_{N_j}^1 h_j^A, \widehat{D}, D_3, \delta_S^2)$，将$\left(M_B, C_S^2\right)$广播给所有认证节点，请求认证节点对签约任务进行认证和提供签约码；同时签约平台S通知用户Bob登录签约平台S查看文书$\widehat{D}$的签署任务；

[0046] S4-12、认证节点$N_t$，t∈{1,2,…,n}随机响应签约平台的请求，决定为对该任务提供认证服务；

[0047] S4-13、签约平台S加密随机参数$r_S^2$和签名$\delta_S^2$，得到密文$C_{S,N_t,1} = Enc(K_t, r_S^2)$，$C_{S,N_t,2} = Enc(K_t, \delta_S^2)$，并将$C_{S,N_t,1}$、$C_{S,N_t,2}$和$C_S^2$发送给响应的认证节点$N_t$；

[0048] S4-14、认证节点$N_t$利用密钥$K_t$解密$C_{S,N_t,1}$和$C_{S,N_t,2}$，获得$r_S^2 = Dec(K_t, C_{S,N_t,1})$，$\delta_S^2 = Dec(K_t, C_{S,N_t,2})$；$N_t$利用$r_S^2$解密$C_S^2$，获得$\widehat{D} = Dec(r_S^2, C_S^2)$；$N_t$将文书$\widehat{D}$存放在随机存储位置$W_{\widehat{D}}$；

[0049] 认证平台$N_t$进行下述计算，获取摘要$D_4$、签名$\delta_{N_t}^1$、签约码$h_t^A$；

[0050] $$D_4 = H(D_3||W_{\widehat{D}}),$$

[0051] $$\delta_{N_t}^1 = sign(SK_{N_t}, D_4),$$

[0052] $h_t^B = H(K_t||r_t^B)$;

[0053] 其中，$r_t^B$为认证节点$N_t$选择的随机参数，认证节点将$(W_{\widehat{D}}, r_t^B)$通过短信发送给Bob，将$(D_4, \delta_{N_t}^1, h_t^B)$发送给签约平台S，认证节点$N_t$利用区块链技术保存

$(S, \widehat{D}, M_B, D_3, \delta_S^2, D_4, \delta_{N_t}^1, W_{\widehat{D}}, h_t^B)$；

[0054] S4-15、签约平台通知Bob确认签约文书；

[0055] S4-16、Bob利用存储位置$W_{\widehat{D}}$查看文书$\widehat{D}$，Bob比对$\widehat{D}$是否与签约平台展示的文书内容一致，如果一致，执行S4-17；否则，签约失败；

[0056] S4-17、Bob在签约平台S输入$r_t^B$；

[0057] S4-18、签约平台S根据Bob输入的随机参数$r_t^B$计算签约码$h_t^{B\prime} = H(K_t||r_t^B)$，判断签约平台计算的签约码与认证节点发送的签约码是否一致，如果$h_t^{B\prime} = h_t^B$等式成立，执行S4-19，否则签署失败；

[0058] S4-19、签约平台S利用Bob身份对文书$\widehat{D}$进行签名，得到文书$\widetilde{D}$，签约平台S进行下述计算，获取摘要$D_5$以及签名$\delta_S^3$；

[0059] $D_5 = H(D_4||\widetilde{D})$,

[0060] $\delta_S^3 = sign(SK_S, D_5)$,

[0061] S利用区块链技术保存$(N_t, D_4, \delta_{N_t}^1, h_t^B, \widetilde{D}, \delta_S^3)$，完成签约。

[0062] 本发明的步骤S3中，签约平台S验证用户注册信息的正确性，对其进行线上或者线下的身份审核。

[0063] 本发明的步骤S4-5和S4-14中，随机存储位置$W_D$和$W_{\widehat{D}}$在对应的认证节点$N_j$和$N_t$上，或者在任何一个或者相应的两个存储平台P上。

[0064] 本发明的各认证节点为各公证处提供的公证存储模块，或者第三方公证存储模块。

[0065] 本发明的步骤S2-3中，密钥共享技术采用认证的Diffie-Hellman密钥交换方法。

[0066] 本发明的步骤S4-1中，Alice利用用户名$U_A$和密码$P_A$登录签约平台S。

[0067] 本发明的步骤S4-4中，签约平台S广播$C_{S,N_j,1}$、$C_{S,N_j,2}$、$C_S^1$给所有的认证节点，对应的步骤4-5中，认证节点$N_j$解密$C_S^1$，获得文书D。

[0068] 本发明的步骤S4-13中，签约平台S广播$C_{S,N_t,1}$、$C_{S,N_t,2}$和$C_S^2$给所有的认证节点，对应的步骤S4-14中，认证节点$N_t$解密$C_S^2$，获得文书$\widehat{D}$。

[0069] 本发明的有益效果：

[0070] 本发明基于区块链技术、外包计算和文书签署技术而提出，相对于传统的文书签署方法，具有如下特点：

[0071] 1、用户不需要保存文书及签名；

[0072] 2、文书签署过程被详细记录，并且不能被篡改；

[0073] 3、用户可以将签署运算外包给签约平台完成；

[0074] 4、多个区块链公证节点的存在可以抵抗签约平台与公证平台的合谋攻击。

## 附图说明

[0075] 图1是本发明的流程图。

## 具体实施方式

[0076] 下面结合附图和实施例对本发明作进一步的说明。

[0077] 如图1所示，一种基于区块链技术的可外包的文书签署方法，采用签约平台和区块链认证节点(认证节点为各公证处提供的公证存储模块，或者第三方公证存储模块)，该方法包括以下步骤：

[0078] S1、系统初始化步骤：

[0079] S1-1、根据安全级别，为签约平台S和区块链认证节点$N_i$选择安全参数γ，i＝1，2，…，n，i表示区块链认证节点的编号，n表示区块链认证节点的总数；

[0080] S1-2、为签约平台S和区块链认证节点$N_i$选择哈希函数H，加密、解密算法(Enc，Dec)；签名、验证算法(Sign，Ver)和密钥产生算法KG；

[0081] S2、秘钥管理系统初始化的步骤：

[0082] S2-1、签约平台S输入安全参数γ，利用密钥产生算法产生S的私钥$SK_S$和公钥$PK_S$，$KG(\gamma)\rightarrow(SK_S,PK_S)$；

[0083] S2-2、各认证节点$N_i$分别输入安全参数γ，利用密钥产生算法产生各自的私钥$SK_{N_i}$和公钥$PK_{N_i}$，$KG(\gamma)\rightarrow(SK_{N_i},PK_{N_i})$；

[0084] S2-3、签约平台S与认证节点$N_i$利用现有密钥交换技术(优选认证的Diffie-Hellman密钥交换方法)交换密钥$K_i$，签约平台保存信息$(N_i,K_i)$，认证平台$N_i$保存信息$K_i$；

[0085] S3、用户注册的步骤：

[0086] 各用户X向签约平台S提交注册信息$ID_X$，并且设置登录密码$P_X$，注册信息$ID_X$包括身份证件号码$IDN_X$、手机号码$M_X$以及用户名$U_X$；签约平台S验证用户注册信息的正确性，对其进行线上或者线下的身份审核；

[0087] S4、用户发起签约的步骤：

[0088] S4-1、Alice利用用户名$U_A$和密码$P_A$登录签约平台S，将文书D导入到签约平台，选择与用户Bob签约；

[0089] S4-2、签约平台S对文书D进行下述计算，得到摘要$D_1$，签名$\delta_S^1$以及加密文书$C_S^1$；

[0090] $D_1=H(D)$，

[0091] $$\delta_S^1=sign(SK_S,\ D_1),$$

[0092] $$C_S^1=Enc(r_s^1,D);$$

[0093] 其中，$r_S^1$表示签约平台的随机参数；

[0094] 签约平台S利用区块链技术保存$(ID_A,\ \mathrm{D},\ D_1,\ \delta_S^1)$，并且将$(M_A,\ \mathrm{C_S^1})$广播给所有认证节点请求认证节点对该任务进行认证和提供认证签约码；

[0095] S4-3、认证节点$N_j$，j∈{1,2,…,n}随机响应签约平台的请求，接受对该签约任务进行认证服务，并就此通知签约平台；

[0096] S4-4、签约平台S加密随机参数$r_S^1$和签名$\delta_S^1$，得到密文$C_{S,N_j,1}=Enc(K_j,\ r_S^1)$，和$C_{S,N_j,2}=Enc(K_j,\ \delta_S^1)$，将$C_{S,N_j,1}$、$C_{S,N_j,2}$、$\mathrm{C_S^1}$发送给响应的认证节点$N_j$；

[0097] S4-5、认证节点$N_j$利用密钥$K_j$解密$C_{S,N_j,1}$、$C_{S,N_j,2}$，获得$r_S^1=Dec(K_j,C_{S,N_j,1})$，$\delta_S^1=Dec(K_j,C_{S,N_j,2})$；$N_j$利用$r_S^1$解密$\mathrm{C_S^1}$，获得$\mathrm{D}=Dec(r_S^1,\ \mathrm{C_S^1})$；$N_j$将文书D存放在随机存储位置$W_D$；前述步骤保证签约平台广播出去的信息，即随机参数和签名只能被相应的节点查看，其他节点看不到广播的内容；

[0098] 认证平台$N_j$进行下述计算，获取摘要$D_1$、$D_2$、签名$\delta_{N_j}^1$、签约码$h_j^A$；

[0099] $D_1=H(D)$，

[0100] $D_2=H(D_1||W_D)$，

[0101] $$\delta_{N_j}^1=sign(SK_{N_j},D_2),$$

[0102] $$h_j^A=H(K_j||r_j^A);$$

[0103] 其中，$r_j^A$为认证节点$N_j$选择的随机参数，认证节点将$(W_D,r_j^A)$通过短信发送给Alice，将$(D_2,\delta_{N_j}^1,h_j^A)$发送给签约平台S；认证节点$N_j$利用区块链技术保存$(\mathrm{S},\mathrm{D},M_A,D_1,\delta_S^1,\ D_2,\delta_{N_j}^1,W_D,h_j^A)$，S表示签约平台的名称；

[0104] S4-6、签约平台通知Alice确认签约文书；

[0105] S4-7、Alice利用访问位置$W_D$查看文书D，Alice比对D是否与原文一致，如果一致，执行S4-8；否则，签约失败；

[0106] S4-8、Alice决定是否签署文书，如果决定签署，执行S4-9；否则，签约终止；

[0107] S4-9、Alice在签约平台S输入$r_j^A$；

[0108] S4-10、签约平台S根据Alice输入的随机参数$r_j^A$计算签约码$h_j^{A\prime}=H(K_j||r_j^A)$，判断签约平台计算的签约码与认证节点发送的签约码是否一致，如果$h_j^{A\prime}=h_j^A$等式成立，执行S4-11，否则签署失败；

[0109] S4-11、签约平台S利用Alice身份对文书D进行签名，得到文书$\widehat{D}$，签约平台S进行下述计算，获取摘要$D_3$，签名$\delta_S^2$以及加密文书$\mathrm{C_S^2}$；

[0110] $$D_3=H(D_2||\widehat{D}),$$

[0111] $\delta_S^2 = sign(SK_S, D_3)$,

[0112] $C_S^2 = Enc(r_s^2, \widehat{D})$;

[0113] 其中，$r_S^2$表示签约平台的随机参数；

[0114] 签约平台S利用区块链技术保存$(N_j, D_2, \delta_{N_j}^1 h_j^A, \widehat{D}, D_3, \delta_S^2)$，将$(M_B, C_S^2)$广播给所有认证节点，请求认证节点对签约任务进行认证和提供签约码；同时签约平台S通知用户Bob登录签约平台S查看文书$\widehat{D}$的签署任务；

[0115] S4-12、认证节点$N_t$，$t \in \{1,2,\cdots,n\}$随机响应签约平台的请求，决定为对该任务提供认证服务；

[0116] S4-13、签约平台S加密随机参数$r_S^2$和签名$\delta_S^2$，得到密文$C_{S,N_t,1} = Enc(K_t, r_S^2)$，$C_{S,N_t,2} = Enc(K_t, \delta_S^2)$，并将$C_{S,N_t,1}$、$C_{S,N_t,2}$和$C_S^2$发送给响应的认证节点$N_t$；

[0117] S4-14、认证节点$N_t$利用密钥$K_t$解密$C_{S,N_t,1}$和$C_{S,N_t,2}$，获得$r_S^2 = Dec(K_t, C_{S,N_t,1})$，$\delta_S^2 = Dec(K_t, C_{S,N_t,2})$；$N_t$利用$r_S^2$解密$C_S^2$，获得$\widehat{D} = Dec(r_S^2, C_S^2)$；$N_t$将文书$\widehat{D}$存放在随机存储位置$W_{\widehat{D}}$；前述步骤保证签约平台广播出去的信息，即随机参数和签名只能被相应的节点查看，其他节点看不到广播的内容；

[0118] 认证平台$N_t$进行下述计算，获取摘要$D_4$、签名$\delta_{N_t}^1$、签约码$h_t^A$；

[0119] $D_4 = H(D_3 || W_{\widehat{D}})$,

[0120] $\delta_{N_t}^1 = sign(SK_{N_t}, D_4)$,

[0121] $h_t^B = H(K_t || r_t^B)$;

[0122] 其中，$r_t^B$为认证节点$N_t$选择的随机参数，认证节点将$(W_{\widehat{D}}, r_t^B)$通过短信发送给Bob，将$(D_4, \delta_{N_t}^1, h_t^B)$发送给签约平台S，认证节点$N_t$利用区块链技术保存$(S, \widehat{D}, M_B, D_3, \delta_S^2, D_4, \delta_{N_t}^1, W_{\widehat{D}}, h_t^B)$；

[0123] S4-15、签约平台通知Bob确认签约文书；

[0124] S4-16、Bob利用存储位置$W_{\widehat{D}}$查看文书$\widehat{D}$，Bob比对$\widehat{D}$是否与签约平台展示的文书内容一致，如果一致，执行S4-17；否则，签约失败；

[0125] S4-17、Bob在签约平台S输入$r_t^B$；

[0126] S4-18、签约平台S根据Bob输入的随机参数$r_t^B$计算签约码$h_t^{B'} = H(K_t || r_t^B)$，判断签约平台计算的签约码与认证节点发送的签约码是否一致，如果$h_t^{B'} = h_t^B$等式成立，执行S4-19，否则签署失败；

[0127] S4-19、签约平台S利用Bob身份对文书$\widehat{D}$进行签名，得到文书$\widetilde{D}$，签约平台S进行下述计算，获取摘要$D_5$以及签名$\delta_S^3$；

[0128] $$D_5 = H\left(D_4||\widetilde{D}\right),$$

[0129] $$\delta_S^3 = sign(SK_S, D_5),$$

[0130] S利用区块链技术保存$(N_t, D_4, \delta_{N_t}^1, h_t^B, \widetilde{D}, \delta_S^3)$，完成签约。

[0131] 本发明的步骤S4-5和S4-14中，随机存储位置$W_D$和$W_{\widehat{D}}$在对应的认证节点$N_j$和$N_t$上，或者在任何一个或者相应的两个存储平台P上。

[0132] 本发明未涉及部分均与现有技术相同或可采用现有技术加以实现。

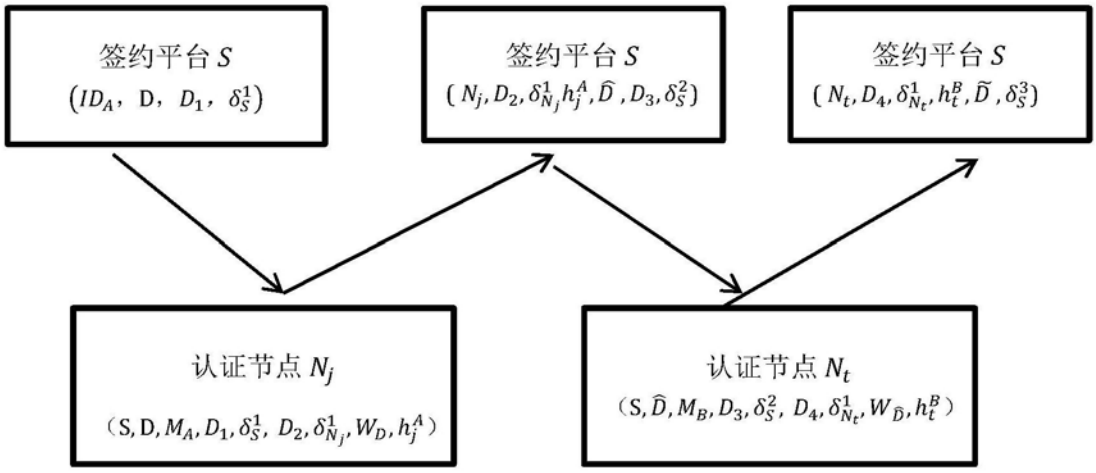

签约平台 $S$
$(ID_A,\ \mathrm{D},\ D_1,\ \delta_S^1)$
签约平台 $S$
$(N_j, D_2, \delta_{N_j}^1 h_j^A, \widehat{D}, D_3, \delta_S^2)$
签约平台 $S$
$(N_t, D_4, \delta_{N_t}^1, h_t^B, \widetilde{D}, \delta_S^3)$
认证节点 $N_j$
$(\mathrm{S}, \mathrm{D}, M_A, D_1, \delta_S^1,\ D_2, \delta_{N_j}^1, W_D, h_j^A)$
认证节点 $N_t$
$(\mathrm{S}, \widehat{D}, M_B, D_3, \delta_S^2,\ D_4, \delta_{N_t}^1, W_{\widehat{D}}, h_t^B)$

图1