(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 114726552 B
(45)授权公告日 2022.10.11

(21)申请号 202210634279.3
(22)申请日 2022.06.07
(65)同一申请的已公布的文献号
申请公布号 CN 114726552 A
(43)申请公布日 2022.07.08
(73)专利权人 杭州天谷信息科技有限公司
地址 310012 浙江省杭州市西湖区西斗门路3号天堂软件园D幢19层
(72)发明人 钟一民 陈传义 郭峰 金宏洲 程亮
(74)专利代理机构 杭州裕阳联合专利代理有限公司 33289
专利代理师 杨琪宇
(51)Int.Cl.
H04L 9/32(2006.01)

(56)对比文件
CN 108259177 A,2018.07.06
CN 1719765 A,2006.01.11
US 2017083867 A1,2017.03.23
JP 2015136049 A,2015.07.27
CN 106789087 A,2017.05.31
CN 114519206 A,2022.05.20
CN 114092076 A,2022.02.25
CN 113849861 A,2021.12.28
肖攸安等.超椭圆曲线可控代理签名方案的研究.《计算机工程与应用》.2006,(第04期),

审查员 程晓青

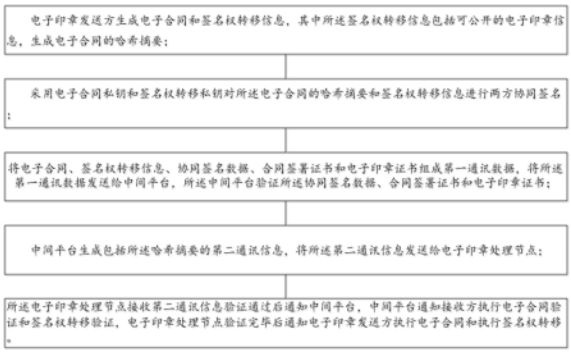
权利要求书2页 说明书6页 附图1页

(54)发明名称

一种数字签名权转移方法和系统

(57)摘要

本发明公开了一种数字签名权转移方法和系统,包括:电子印章发送方生成电子合同和签名权转移信息,其中所述签名权转移信息包括可公开的电子印章信息,生成电子合同的哈希摘要;采用电子合同私钥和签名权转移私钥对所述电子合同的哈希摘要和签名权转移信息进行两方协同签名;将电子合同、签名权转移信息、协同签名数据、合同签署证书和电子印章证书组成第一通讯数据,将所述第一通讯数据发送给中间平台,所述中间平台验证所述协同签名数据、合同签署证书和电子印章证书;中间平台在接收到发送方电子印章处理节点验证通过后通知接收方验证,所有电子印章所有方均完成签署后,由中间平台通知电子印章处理节点执行签名权转移和合同相关事务。



CN 114726552 B

1.一种数字签名权转移方法,其特征在于,所述方法包括如下步骤:

电子印章发送方生成电子合同和签名权转移信息,所述电子合同用于约束签名权转移,其中所述签名权转移信息包括可公开的电子印章信息,生成电子合同的哈希摘要;

采用电子合同私钥和签名权转移私钥对所述电子合同的哈希摘要和签名权转移信息进行两方协同签名;

将电子合同、签名权转移信息、协同签名数据、合同签署证书和电子印章证书组成第一通讯信息,将所述第一通讯信息发送给中间平台,所述中间平台验证所述协同签名数据、合同签署证书和电子印章证书;

中间平台生成包括所述哈希摘要的第二通讯信息,将所述第二通讯信息发送给电子印章处理节点;

所述电子印章处理节点接收第二通讯信息验证通过后通知中间平台,中间平台通知接收方执行电子合同验证和签名权转移验证,电子印章处理节点验证完毕后通知电子印章发送方执行电子合同和执行签名权转移。

2.根据权利要求1所述的一种数字签名权转移方法,其特征在于,所述签名权转移信息包括:电子印章发送方信息、电子印章接收方信息,电子印章转移时间戳和可公开的电子印章信息,其中所述电子印章信息包括电子印章私钥、电子印章图片和电子印章证书,其中所述电子印章私钥为不可公开信息,电子印章图片和电子印章证书为可公开信息。

3.根据权利要求1所述的一种数字签名权转移方法,其特征在于,所述中间平台对签名权转移信息进行验证方法包括:

获取电子印章发送方的第一通讯信息,获取所述第一通讯信息的签名权转移信息、协同签名数据、合同签署证书和电子印章证书;

获取合同哈希摘要验证所述协同签名数据,将验证通过后的所述合同哈希摘要、签名权转移信息、协同签名数据、合同签署证书和电子印章证书组合生成第二通讯信息,并将所述第二通讯信息发送给电子印章处理节点;

所述电子印章处理节点分别验证所述签名权转移信息、协同签名数据、合同签署证书和电子印章证书。

4.根据权利要求1所述的一种数字签名权转移方法,其特征在于,所述电子印章处理节点对所述签名权转移信息验证方法包括:获取签名权转移信息中的时间戳、发送方信息、接收方信息、电子印章信息;

分别验证时间戳是否合理、发送方信息和接收方信息是否合理、发送方的电子印章信息否满足签名权转移信息要求;

验证通过后发送验证通过消息通知所述中间平台。

5.根据权利要求1所述的一种数字签名权转移方法,其特征在于:

所述电子合同包括:签名权转移的时间、地点、转移双方的身份、转移的目的、转移双方的权利义务、转移的时间期限与当前签名权转移有关且具有法律意义的信息。

6.根据权利要求1所述的一种数字签名权转移方法,其特征在于:

所述中间平台在获取到所述第一通讯信息后,进一步验证所述第一通讯信息的合同签署证书和电子印章证书,并根据所述签名权转移信息和电子印章证书判断当前电子印章的归属和目标转移对象是否正确。

7.根据权利要求1所述的一种数字签名权转移方法,其特征在于:

所述中间平台在获取到所述第一通讯信息后,先验证所述合同签署证书和电子印章证书,证书验证通过后,进一步利用两方协同签名算法验证所述协同签名数据,协同签名数据验证通过后,进一步验证所述签名权转移信息的合理性。

8.根据权利要求1所述的一种数字签名权转移方法,其特征在于:

当所述中间平台在完成所述第一通讯信息的证书验证、协同签名验证和签名权转移信息合理性验证并通过后,所述中间平台将第一通讯信息发送给接收方,接收方确认电子合同和电子印章信息无误后执行两方协同签名,生成接收方的协同签名数据,其中所述协同签名数据采用接收方自身的电子合同私钥和签名权转移私钥,将接收方验证通过的信息与接收方的合同签署证书和协同签名数据发送给中间平台,所述中间平台验证接收方的合同签署证书和协同签名数据并通过后,将发送方和接收方验证通过的信息组装后发送给电子印章处理节点,电子印章处理节点验证通过后通知发送方执行电子印章的转移,所述电子印章处理节点在完成电子印章转移过程中生成新的电子印章信息并对电子印章内的已有电子印章信息进行替换。

9.一种数字签名权转移系统,其特征在于,所述系统执行权利要求1-8中任意一项所述的一种数字签名权转移方法。

10.一种计算机可读存储介质,其特征在于,计算机可读存储介质存储有计算机程序,所述计算机程序可被处理器执行权利要求1-8中任意一项所述的一种数字签名权转移方法。

一种数字签名权转移方法和系统

技术领域

[0001] 本发明涉及数字签名技术领域,特别涉及一种数字签名权转移方法和系统。

背景技术

[0002] 电子签名已经越来越被企业和个人所熟知并运用,而且也是互联网发展的必然趋势。电子签名带来的诸多好处让企业用户们颇为认可,不但管理方便而且节约很大一部分成本,同时具有法律保障。

[0003] 当前电子签名在企业应用中,往往配备专用的电子签名硬件,例如UKEY等,该类硬件往往还带有印章图片,成为电子印章。盖章时,将印章图片放入文档的指定位置,并用电子印章的私钥对文档签名,则形成了带电子签章的文档,具备法律效力。

[0004] 现有技术中电子签名的存在的技术缺陷包括:1、现有技术中,拥有电子印章即拥有签名权,如电子印章丢失将造成严重的后果;2、如电子印章需要转移,即签名权由A转为B,只需要将电子印章进行转交,不具备法律效力,容易引起事后争议,且难以取证。

发明内容

[0005] 本发明其中一个发明目的在于提供一种数字签名权转移方法和系统,所述方法和系统利用中间平台对电子印章的转移过程全程记录,因此在签名权转移的过程中具有可追溯查询的功能,并且电子印章只要一次通信流程即可完成签名权转移,无需分为电子合同签署、电子印章转移两个流程,提高数字签名权转移的效率。

[0006] 本发明另一个发明目的在于提供一种数字签名权转移方法和系统,所述方法和系统通过中间平台在签名权转移验证完毕后,将电子印章转移的业务由中间平台通知,因此不会向电子印章处理节点暴露更多的比如转移双方的身份、转移的目的、转移双方的权利义务、转移的时间期限等敏感信息,从而提高签名权转移的安全性。

[0007] 本发明另一个发明目的在于提供一种数字签名权转移方法和系统,所述方法和系统采用双私钥协同签名,即对合同或其他签名文件的签名需要两个私钥,且其中一个私钥是电子合同签名私钥,该电子合同签名私钥保存于通讯方的终端中,另一个是签名权转移私钥,该签名权转移私钥保存于电子印章硬件中,由于该电子合同所需的两个签名私钥并不保存于同一设备内,避免非法签名签署方在电子印章丢失或被盗后进行非法签名的风险。

[0008] 为了实现至少一个上述发明目的,本发明进一步提供一种数字签名权转移方法,所述方法包括如下步骤:

[0009] 电子印章发送方生成电子合同和签名权转移信息,其中所述签名权转移信息包括可公开的电子印章信息,生成电子合同的哈希摘要;

[0010] 采用电子合同私钥和签名权转移私钥对所述电子合同的哈希摘要和签名权转移信息进行两方协同签名;

[0011] 将电子合同、签名权转移信息、协同签名数据、合同签署证书和电子印章证书组成

第一通讯信息，将所述第一通讯信息发送给中间平台，所述中间平台验证所述协同签名数据、合同签署证书和电子印章证书；

[0012] 中间平台生成包括所述哈希摘要的第二通讯信息，将所述第二通讯信息发送给电子印章处理节点；

[0013] 所述电子印章处理节点接收第二通讯信息验证通过后通知中间平台，中间平台通知接收方执行电子合同验证和签名权转移验证，电子印章处理节点验证完毕后通知电子印章发送方执行电子合同和执行签名权转移。

[0014] 根据本发明另一个较佳实施例，所述签名权转移信息包括：电子印章发送方信息、电子印章接收方信息，电子印章转移时间戳和可公开的电子印章信息，其中所述电子印章信息包括电子印章私钥、电子印章图片和电子印章证书，其中所述电子印章私钥不可公开，其他电子印章信息可公开。

[0015] 根据本发明其中一个较佳实施例，所述中间平台对签名权转移信息进行验证方法包括：

[0016] 获取电子印章发送方的第一通讯信息，获取所述第一通讯信息的签名权转移信息、协同签名数据、合同签署证书和电子印章证书；

[0017] 获取合同哈希摘要验证所述协同签名数据，验证通过后的所述合同哈希摘要、签名权转移信息、协同签名数据、合同签署证书和电子印章证书组合生成第二通讯信息，并将所述第二通讯信息发送给电子印章处理节点；

[0018] 所述电子印章处理节点分别验证所述签名权转移信息、协同签名数据、合同签署证书和电子印章证书。

[0019] 根据本发明另一个较佳实施例，所述电子印章处理节点对所述签名权转移信息验证方法包括：获取签名权转移信息中的时间戳、发送方信息、接收方信息、电子印章信息；

[0020] 分别验证时间戳是否合理、发送方信息和接收方信息是否合理、发送方的电子印章信息是否满足签名权转移信息要求；

[0021] 验证通过后发送验证通过消息通知所述中间平台。

[0022] 根据本发明另一个较佳实施例，所述电子合同包括：签名权转移的时间、地点、转移双方的身份、转移的目的、转移双方的权利义务、转移的时间期限与当前签名权转移有关且具有法律意义的信息。

[0023] 根据本发明另一个较佳实施例，所述中间平台在获取到所述第一通讯信息后，进一步验证所述第一通讯信息的合同签署证书和电子印章证书，并根据所述签名权转移信息和电子印章证书判断当前电子印章的归属和目标转移对象是否正确。

[0024] 根据本发明另一个较佳实施例，所述中间平台在获取到所述第一通讯信息后，先验证所述合同签署证书和电子印章证书，证书验证通过后，进一步利用两方协同签名算法验证所述协同签名数据，协同签名数据验证通过后，进一步验证所述签名权转移信息的合理性。

[0025] 根据本发明另一个较佳实施例，当所述中间平台在完成所述第一通讯信息的证书验证、协同签名验证和签名权转移信息合理性验证并通过后，所述中间平台将第一通讯信息发送给接收方，接收方确认电子合同和电子印章信息无误后执行两方协同签名，生成接收方的协同签名数据，其中所述协同签名数据采用接收方自身的电子合同私钥和签名权转

移私钥,将接收方验证通过的信息与接收方的合同签署证书和协同签名数据发送给中间平台,所述中间平台验证接收方的合同签署证书和协同签名数据并通过后,将发送方和接收方验证通过的信息组装后发送给电子印章处理节点,电子印章处理节点验证通过后通知发送方执行电子印章的转移,所述电子印章处理节点在完成电子印章转移过程中生成新的电子印章信息并对电子印章内的已有电子印章信息进行替换。

[0026] 为了实现至少一个上述发明目的,本发明进一步提出一种数字签名权转移系统,所述系统执行上述一种数字签名权转移方法。

[0027] 本发明进一步提供一种计算机可读存储介质,计算机可读存储介质存储有计算机程序,所述计算机程序可被处理器执行所述一种数字签名权转移方法。

附图说明

[0028] 图1显示的是本发明一种数字签名权转移方法的流程示意图。

[0029] 图2显示的是本发明一种数字签名权转移系统结构示意图。

具体实施方式

[0030] 以下描述用于揭露本发明以使本领域技术人员能够实现本发明。以下描述中的优选实施例只作为举例,本领域技术人员可以想到其他显而易见的变型。在以下描述中界定的本发明的基本原理可以应用于其他实施方案、变形方案、改进方案、等同方案以及没有背离本发明的精神和范围的其他技术方案。

[0031] 可以理解的是,术语“一”应理解为“至少一”或“一个或多个”,即在一个实施例中,一个元件的数量可以为一个,而在另外的实施例中,该元件的数量可以为多个,术语“一”不能理解为对数量的限制。

[0032] 请结合图1和图2,本发明公开了一种数字签名权转移方法和系统,其中所述方法包括如下步骤:电子印章发送方根据事务需要生成电子合同数据和签名权转移信息。定义发送方为U,发送方对应的电子合同数据为C,发送方对应的电子签名权转移信息为CTX,其中所述签名权转移信息CTX包括:时间戳、发送方信息(U)、接收方信息和可公开电子印章信息,其中电子印章信息包括当前电子印章的电子印章私钥,电子印章图片、电子印章证书以及电子印章的所有者等。其中所述电子印章私钥为不可公开信息,其他均为可公开信息。所述接收方信息包括合同的签署方即签名权转移对象,其中本发明还需要一个中间平台S,所述中间平台可以接收所述签名权转移的事务信息CTX,并将所述签名权转移事务信息CTX发送给对应的电子印章处理节点。

[0033] 所述发送方U同时也是合同的签署方,当所述发送方U生成所述电子签名转移信息CTX后,进一步计算所述电子合同数据C的哈希摘要,并对所述哈希摘要和签名权转移信息HASH(C)||CTX进行协同签名。其中所述协同签名为两方协同签名,两方协同签名算法可根据现有技术《Damgard I , Mikkelsen G L , Skeltved T . On the security of distributed multiprime RSA.[C]// International Conference on Information Security and Cryptology. 2014》建立,因此本发明对如何实现两方协同签名不再赘述,且不限于上述论文所述方法。值得一提的是,本发明采用双私钥的协同签名,其中一个私钥是每个签名方自身的电子合同私钥,而另一个私钥是电子印章的签名权转移私钥,电子印

章的签名权转移私钥优选为电子印章的私钥，采用所述电子合同私钥和签名权转移私钥对所述哈希摘要和事务信息进行所述两方协同签名，获取发送方的协同签名数据CSIGU。

[0034] 所述发送方根据获取的协同签名数据、合同数据、签名权转移信息、合同签署证书和电子印章证书，生成包含上述数据和证书的第一通讯信息：MSGU=C||CTX||CSIGU||CERTU||CERTW，其中CERTU为发送方用于电子合同签署的证书，简称为合同签署证书，CERTW为发送方用于电子印章的签名权转移的电子印章证书，所述电子印章证书由电子印章处理节点WS所颁发，其载体是一种实体密码学硬件装置。

[0035] 所述发送方将所述第一通讯信息发送给中间平台S，所述中间平台S在获取所述第一通讯信息后进一步验证所述第一通讯信息包含的合同数据和签名权转移信息。其中所述中间平台S获取所述第一通讯信息中的合同签署证书和电子印章证书，且所述中间平台S验证所述合同签署证书和电子印章证书，判断电子印章的种类，其中证书验证为现有技术，本发明对如何验证数字证书不再详细描述。在完成所述合同签署证书和电子印章证书的验证后，计算所述第一通讯信息中的哈希摘要，并对所述协同签名进行验证，采用两方协同签名算法对应的验证算法验证所述签名，需要说明的是，所述验证算法为现有技术，本发明对此不再赘述。由于签名权转移中需要同时拥有电子合同私钥和数字签名权转移私钥才能进行签名和事务处理，因此可以大幅降低私钥丢失或被盗窃后电子印章被非法使用的可能性，保障签名权转移的安全性。

[0036] 所述中间平台进一步验证签名权转移信息，其中所述签名权转移信息的验证方法包括：获取计算的所述哈希摘要HASH(C)，将所述哈希摘要和签名权转移信息、协同签名数据、合同签署证书和电子印章证书一同组合生成第二通讯信息，所述第二通讯信息包含电子签名转移信息DTX=HASH(C)||CTX||CSIGU||CERTU||CERTW，将所述第二通讯信息发送给对应的电子印章处理节点WS，由于向所述电子印章处理节点发送的是哈希摘要HASH(C)，因此不会在所述电子印章处理节点上暴露相关的合同信息，所述电子印章处理节点对获取的第二通讯信息中的合同签署证书CERTU和电子印章证书CERTW进行验证，验证完毕后进一步对所述第二通讯信息中的协同签名数据CSIGU进行验证，完成所述协同签名数据CSIGU验证后进一步验证所述签名权转移信息，其中所述签名权转移信息的验证包括但不仅限于：对时间合理性的验证(例如是否是刚刚发生，以确保不是历史消息的重放)、对发送方信息合理性的验证(例如是否与CERTU中一致、单独对发送方进行身份认证和意愿认证等)、对接收方信息合理性的验证(例如接收方是否存在、接收方是否可以作为电子印章的主人、单独对接收方进行身份认证和意愿认证等)、对电子印章信息合理性的验证(例如电子印章是否可更换主人、当前主人是否为电子印章所有人)等。当所述电子印章处理节点完成上述验证并通过后，向所述中间平台发送验证通过消息，或验证不通过则返回对应的错误消息。上述验证过程并不存在实际电子印章的签名权转移处理过程。

[0037] 所述中间平台获取电子印章处理节点的验证信息后，中间平台对合同数据、签名权转移信息、协同签名数据、合同签署证书和电子印章证书C||CTX||CSIGU||CERTU||CERTW组成中间平台的验证通过通知消息，所述验证通过通知消息发送给签名权转移信息中记载的接收方，接收方在获取验证通过通知消息后分别执行合同的签署操作，其中所述合同签署操作包括：计算哈希摘要HASH(C)，由于合同数据是相同的，因此相对于发送方的哈希摘要是相同的。并将所述接收方的签名权转移信息CTX和所述哈希摘要采用电子合同私钥和

签名权转移私钥进行两方协同签名,生成对应的接收方签名信息。在完成签名后生成和所述第一通讯信息相同数据类型的通讯信息发送给所述中间平台,所述中间平台进一步执行接收方的签名的验证,所述中间平台接收到接收方签名验证通过消息后,所述中间平台向所述电子印章处理节点发送签名权转移执行信息,所述电子印章处理节点将执行合同对应的签名权转移。使得发送方和接收方的电子印章信息发生变化,并将变化记录保存。

[0038] 具体而言,当所述中间平台S将所述第一通讯信息中的签名权转移信息验证完毕后,将所述第一通讯信息MSGU保存后转发给接收方(V),并向所述接收方发送验证完毕的签名权转移信息CTX,接收方在判断合同和电子印章信息无误后,接收方利用自身的电子合同私钥和签名权转移私钥进行两方协同签名和合同签署,生成接收方的两方协同签名数据CSIGV和合同签署证书CERTV,接收方将两方协同签名数据CSIGV和合同签署证书CERTV发送给中间平台S,中间平台S在获取到所述两方协同签名数据CSIGV和合同签署证书CERTV后,进一步将发送方和接收方验证通过信息组装生成验证完毕的信息DTX'=HASH(C)||CTX||CSIGU||CSIGV||CERTU||CERTV||CERTW,并将所述验证完毕的信息发送给电子印章处理节点,所述电子印章处理节点对每个两方协同签名数据、合同签署证书、电子印章信息、电子印章证书和哈希摘要进行验证,验证通过后,通知印章所有方向对应的接收方转移印章。并且所述印章处理节点还生成新的电子印章信息。新的电子印章信息包含:新的印章私钥、印章图片、印章证书,其中新的印章证书中包含新主人V,并删除上一主人U;特别地,私钥及证书中的公钥可以不改,印章图片也可以不改,并在本地进行记录,并将其用电子印章的公钥加密传输到电子印章内部,且该消息带有电子印章处理节点WS的签名,电子印章接收后首先验证电子印章处理节点WS的签名,然后用电子印章的私钥解密信息并存储,最后销毁旧的电子印章信息(含旧的印章私钥、印章图片、印章证书);电子印章处理节点WS完成实际的电子印章转移事务后通知中间平台S,中间平台S对合同的转移事务情况进行记录,并记录合同状态为执行完成,此时签名权得到完整移交。如当事双方后续对本次数字签名权的转移存在任何异议,可在中间平台获取合同及相关事务的存证。

[0039] 特别地,根据本发明公开的实施例,上文参考流程图描述的过程可以被实现为计算机软件程序。例如,本公开的实施例包括一种计算机程序产品,其包括承载在计算机可读介质上的计算机程序,该计算机程序包含用于执行流程图所示的方法的程序代码。在这样的实施例中,该计算机程序可以通过通信部分从网络上被下载和安装,和/或从可拆卸介质被安装。在该计算机程序被中央处理单元(CPU)执行时,执行本申请的方法中限定的上述功能。需要说明的是,本申请上述的计算机可读介质可以是计算机可读信号介质或者计算机可读存储介质或者是上述两者的任意组合。计算机可读存储介质例如可以是但不限于电、磁、光、电磁、红外线段、或半导体的系统、装置或器件,或者任意以上的组合。计算机可读存储介质的更具体的例子可以包括但不限于:具有一个或多个导线段的电连接、便携式计算机磁盘、硬盘、随机访问存储器(RAM)、只读存储器(ROM)、可擦式可编程只读存储器(EPROM或闪存)、光纤、便携式紧凑磁盘只读存储器(CD-ROM)、光存储器件、磁存储器件、或者上述的任意合适的组合。在本申请中,计算机可读存储介质可以是任何包含或存储程序的有形介质,该程序可以被指令执行系统、装置或者器件使用或者与其结合使用。而在本申请中,计算机可读的信号介质可以包括在基带中或者作为载波一部分传播的数据信号,其中承载了计算机可读的程序代码。这种传播的数据信号可以采用多种形式,包括但不限于电磁信

号、光信号或上述的任意合适的组合。计算机可读的信号介质还可以是计算机可读存储介质以外的任何计算机可读介质，该计算机可读介质可以发送、传播或者传输用于由指令执行系统、装置或者器件使用或者与其结合使用的程序。计算机可读介质上包含的程序代码可以用任何适当的介质传输，包括但不限于：无线段、电线段、光缆、RF等等，或者上述的任意合适的组合。

[0040] 附图中的流程图和框图，图示了按照本发明各种实施例的系统、方法和计算机程序产品的可能实现的体系架构、功能和操作。在这点上，流程图或框图中的每个方框可以代表一个模块、程序段、或代码的一部分，该模块、程序段、或代码的一部分包含一个或多个用于实现规定的逻辑功能的可执行指令。也应当注意，在有些作为替换的实现中，方框中所标注的功能也可以以不同于附图中所标注的顺序发生。例如，两个接连地表示的方框实际上可以基本并行地执行，它们有时也可以按相反的顺序执行，这依所涉及的功能而定。也要注意的是，框图和/或流程图中的每个方框、以及框图和/或流程图中的方框的组合，可以用执行规定的功能或操作的专用的基于硬件的系统来实现，或者可以用专用硬件与计算机指令的组合来实现。

[0041] 本领域的技术人员应理解，上述描述及附图中所示的本发明的实施例只作为举例而并不限制本发明，本发明的目的已经完整并有效地实现，本发明的功能及结构原理已在实施例中展示和说明，在没有背离所述原理下，本发明的实施方式可以有任何变形或修改。

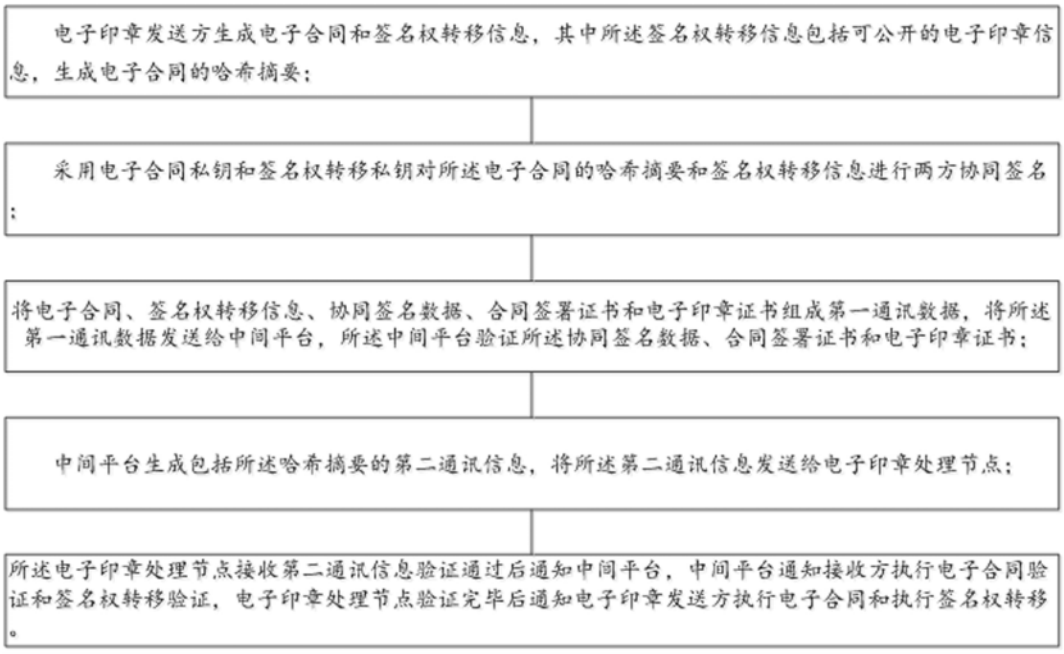

电子印章发送方生成电子合同和签名权转移信息，其中所述签名权转移信息包括可公开的电子印章信息，生成电子合同的哈希摘要；
采用电子合同私钥和签名权转移私钥对所述电子合同的哈希摘要和签名权转移信息进行两方协同签名；
将电子合同、签名权转移信息、协同签名数据、合同签署证书和电子印章证书组成第一通讯数据，将所述第一通讯数据发送给中间平台，所述中间平台验证所述协同签名数据、合同签署证书和电子印章证书；
中间平台生成包括所述哈希摘要的第二通讯信息，将所述第二通讯信息发送给电子印章处理节点；
所述电子印章处理节点接收第二通讯信息验证通过后通知中间平台，中间平台通知接收方执行电子合同验证和签名权转移验证，电子印章处理节点验证完毕后通知电子印章发送方执行电子合同和执行签名权转移。

图1

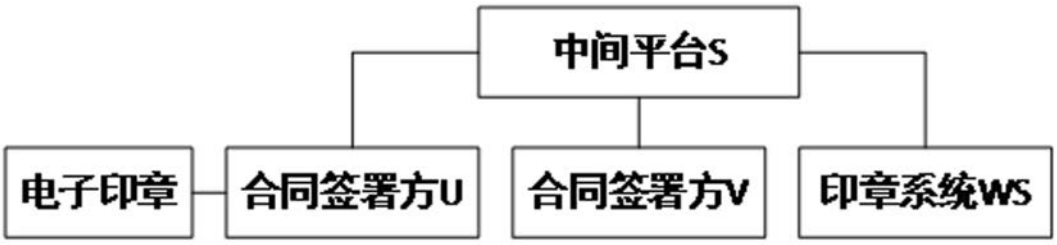

中间平台S
电子印章
合同签署方U
合同签署方V
印章系统WS

图2