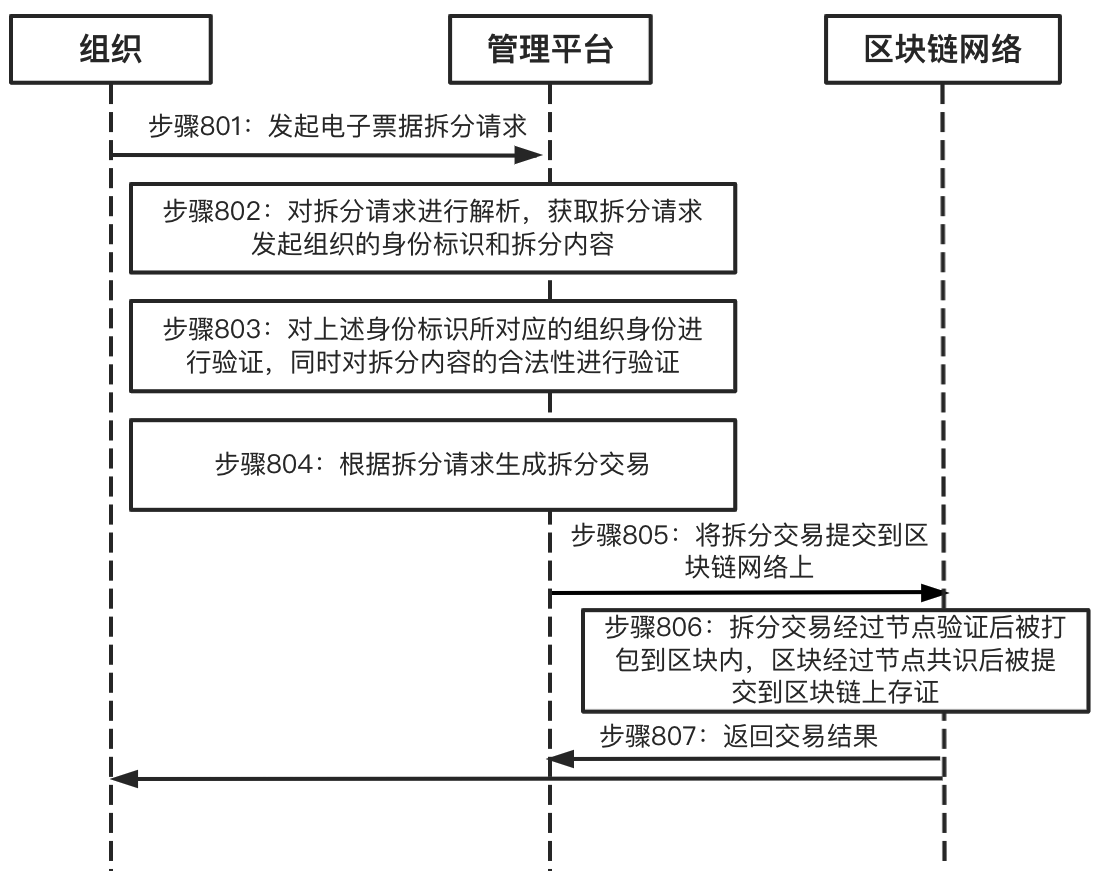
说 明 书 摘 要

GG221116182A

本申请公开了一种基于区块链的电子票据拆分、查询方法及装置，包括发起电子票据拆分请求；对拆分请求进行解析，获取拆分请求发起组织的身份标识和拆分内容；对身份标识所对应的组织身份进行验证，同时对拆分内容的合法性进行验证；根据拆分请求生成拆分交易，并提交到区块链网络上；拆分交易经过节点验证被打包到区块内，经过节点共识后被提交到区块链上存证；向拆分请求的发起组织和管理平台返回交易结果，管理平台将拆分交易和交易结果持久化存储。本发明能够将供应链在不同阶段产生的电子票据信息和交易信息存证到区块链上，实现电子票据的灵活拆分，保证电子票据的流转记录公开验证性和不可篡改性，有效促进电子票据在供应链中的流转。

摘 要 附 图

GG221116182A

****

权 利 要 求 书

GG221116182A

1.一种基于区块链的电子票据拆分方法，应用于管理平台，其特征在于，所述方法包括：

获取组织发起的电子票据拆分请求；

对拆分请求进行解析，获取拆分请求发起组织的身份标识和拆分内容；

对所述身份标识进行组织身份验证，同时对所述拆分内容进行合法性验证；

在组织身份验证及合法性验证通过后，根据所述拆分请求生成拆分交易，并提交到区块链网络上；

获取所述区块链网络所返回的交易结果；其中，所述交易结果是在区块链网络中通过将所述拆分交易经过节点验证打包到区块内，并经过节点共识后被提交到区块链上存证后得到。

2.根据权利要求1所述的方法，其特征在于，对所述身份标识进行组织身份验证，包括：

当所述拆分请求上的身份标识与管理平台内的原始信息相匹配时，通过数字签名确定所述拆分请求的发起者的身份信息。

其中，所述身份标识可以是所述拆分请求发起组织系统节点的公钥，管理平台内的原始信息可以是组织申请准入系统时平台为其颁发的数字证书相关信息，使用数字证书即可确定组织身份，通过密码学原理使用数字证书中包含的组织公钥对数字签名的合法性进行验证，可以确定上述拆分请求的发起者的身份信息。

3.根据权利要求1所述的方法，其特征在于，对所述拆分内容进行合法性验证，包括：

对拆分内容中所述待拆分电子票据的存在性验证，待拆分电子票据的存在性验证可以通过待拆分电子票据的FROM\_PATH字段来完成；FROM\_PATH字段是所述待拆分电子票据在TreeLink中的存储路径，通过FROM\_PATH字段，可以快速定位所述待拆分电子票据在TreeLink中的位置。

4.根据权利要求1所述的方法，其特征在于，根据所述拆分请求生成拆分交易，包括：

管理平台根据拆分请求中的拆分内容，产生多个随机数，随机数的数量和票据拆分目标产生的子票据的数量相同，分别对多个随机数和上述待拆分电子票据的ID哈希，生成多个待产生电子票据的编号，管理平台分别把上述随机数和对应产生的编号添加到拆分请求上，并使用平台私钥进行数字签名，生成拆分交易。

5.根据权利要求1所述的方法，其特征在于，区块经过节点共识后被提交到区块链上存证，包括：

节点对拆分交易上的数字签名进行验证；其中，拆分交易在区块链网络上存证是指拆分交易所产生的电子票据信息和交易全流程的秘密存证。

6.根据权利要求1所述的方法，其特征在于，获取所述区块链网络所返回的交易结果，包括：

发起组织的身份标识，上述拆分交易所拆分产生的新电子票据信息。

其中，所述区块链网络内共识上链的区块中所包含的交易信息和电子票据信息都是以哈希摘要的形式存储的，同时，管理平台在本地或者云端数据库以公钥加密的形式存储所述交易信息和电子票据信息。可以理解地，这么做的目的是通过链上的哈希摘要，对管理平台上存储的票据信息进行准确性校验，防止遭到第三方篡改。

7.一种基于区块链的电子票据查询方法，应用于管理平台，其特征在于，所述方法包括：

获取组织发起的电子票据查询请求，对查询请求进行解析，获取查询请求发起组织的组织标识和查询内容；所述查询内容包括电子票据信息；

根据所述组织标识，获取管理平台中的组织权限信息；并对所述组织权限信息与所述查询请求中所需要的权限信息进行校验；

当所述组织权限信息与所述查询请求中的权限信息相匹配时，在管理平台中获取相应的电子票据信息；

将所获取的相应的电子票据信息向查询请求发起组织进行推送。

8.根据权利要求7所述的方法，其特征在于，当所述组织权限信息与所述查询请求中的权限信息相匹配时，在管理平台中获取相应的电子票据信息，包括：

获取查询请求中的查询条件信息；通过查询请求中的组织标识确定组织身份；在管理平台中获取组织的权限信息，确定组织身份对应的权限是否可执行上述查询请求。

组织权限信息与查询请求中所需要的权限信息相匹配时，通过查询请求中的组织身份标识确定组织公钥；使用组织公钥对区块链网络中获取到的相应的电子票据信息进行加密处理，得到查询请求中的电子票据信息的加密信息。

9.根据权利要求7所述的方法，其特征在于，所述方法还包括：

所述组织权限信息与所述查询请求中所需要的权限信息不匹配时，向组织返回错误消息，即所述组织不具有上述电子票据信息的查询权限。

10.根据权利要求7所述的方法，其特征在于，在管理平台中获取相应的电子票据信息，包括：

获取所述查询请求中的查询条件信息，所述查询条件信息包括至少一个目标维度的目标索引；根据所述至少一个目标维度的目标索引值，查询所述管理平台中的信息索引表，得到所述电子票据信息，其中，信息索引表包括已存储电子票据信息的组织标识以及不同维度的索引值。

11.根据权利要求7所述的方法，其特征在于，将所获取的相应的电子票据信息向查询请求发起组织进行推送，包括：

将所获取的相应的电子票据信息向相应的组织进行推送，其中，电子票据信息为加密信息，组织使用加密使用的公钥对应的私钥进行解密获取到相应的电子票据信息的明文。链上票据的哈希摘要信息是在每个组织本地存储的，组织可以通过摘要信息对获取到的电子票据进行正确性检验。

12.一种基于区块链的电子票据拆分装置，其特征在于，所述装置包括：

获取模块，用于获取组织发起的电子票据拆分请求；

解析模块，用于对拆分请求进行解析，获取拆分请求发起组织的身份标识和拆分内容；

验证模块，用于对所述身份标识进行组织身份验证，同时对所述拆分内容进行合法性验证；

处理模块，用于在组织身份验证及合法性验证通过后，根据所述拆分请求生成拆分交易，并提交到区块链网络上；

传输模块，用于获取所述区块链网络所返回的交易结果；其中，所述交易结果是在区块链网络中通过将所述拆分交易经过节点验证打包到区块内，并经过节点共识后被提交到区块链上存证后得到。

13.一种基于区块链的电子票据查询装置，其特征在于，所述查询装置包括：

获取模块，获取组织发起的电子票据查询请求，对查询请求进行解析，获取查询请求发起组织的组织标识和查询内容；所述查询内容包括电子票据信息；

校验模块，根据所述组织标识，获取管理平台中的组织权限信息；并对所述组织权限信息与所述查询请求中所需要的权限信息进行校验；

处理模块，当所述组织权限信息与所述查询请求中的权限信息相匹配时，在管理平台中获取相应的电子票据信息；

传输模块，将所获取的相应的电子票据信息向查询请求发起组织进行推送。

说 明 书

GG221116182A

一种基于区块链的电子票据拆分、查询方法及装置

技术领域

本发明涉及区块链技术领域，特别涉及一种基于区块链的电子票据拆分、查询方法及装置。

背景技术

现有技术中，传统的电子票据系统中都是采用纸票的形式来流通管理，纸质票据在流通过程中面临着诸多难题，如拆分困难，鉴别困难，交易繁琐，票据保管难等等，即便已经在推进电子票据，一般也都是由各个金融机构内部发行的电子票据，然后汇总到统一的信息平台，最后再开放给其他企业查询访问。因此，传统的电子票据管理系统仍然是一个中心化的票据系统，可能会造成其他企业对系统数据的不信任，而且由于数字信息的可克隆性强，难以灵活拆分，这在涉及多层供应商的供应链金融系统中是非常不便的。

供应链中往往涉及多家企业，电子票据的流转过程中无法总是单个满足业务需求，大多数情况下需要对电子票据进行拆分。同时，供应链中的核心企业或金融机构成为链上交易信息的实际控制者，造成了各级企业对票据信息和交易信息控制能力的不对等，从而使得供应链上的数据信息无法公开验证，这对供应链系统中电子票据的应用造成了严重的阻碍。

发明内容

基于此，本申请实施例提供了一种基于区块链的电子票据拆分、查询方法及装置，可实现灵活拆分的同时，保证电子票据信息的不可篡改性，有效提高信息安全，为数字资产在供应链中自由快速流动提供保障。

第一方面，提供了一种基于区块链的电子票据拆分方法，应用于管理平台，该方法包括：

获取组织发起的电子票据拆分请求；

对拆分请求进行解析，获取拆分请求发起组织的身份标识和拆分内容；

对所述身份标识进行组织身份验证，同时对所述拆分内容进行合法性验证；

在组织身份验证及合法性验证通过后，根据所述拆分请求生成拆分交易，并提交到区块链网络上；

获取所述区块链网络所返回的交易结果；其中，所述交易结果是在区块链网络中通过将所述拆分交易经过节点验证打包到区块内，并经过节点共识后被提交到区块链上存证后得到。

可选地，对所述身份标识进行组织身份验证，包括：

当所述拆分请求上的身份标识与管理平台内的原始信息相匹配时，通过数字签名确定所述拆分请求的发起者的身份信息。

其中，所述身份标识可以是所述拆分请求发起组织系统节点的公钥，管理平台内的原始信息可以是组织申请准入系统时平台为其颁发的数字证书相关信息，使用数字证书即可确定组织身份，通过密码学原理使用数字证书中包含的组织公钥对数字签名的合法性进行验证，可以确定上述拆分请求的发起者的身份信息。

可选地，对所述拆分内容进行合法性验证，包括：

对拆分内容中所述待拆分电子票据的存在性验证，待拆分电子票据的存在性验证可以通过待拆分电子票据的FROM\_PATH字段来完成；FROM\_PATH字段是所述待拆分电子票据在TreeLink中的存储路径，通过FROM\_PATH字段，可以快速定位所述待拆分电子票据在TreeLink中的位置。

可选地，根据所述拆分请求生成拆分交易，包括：

管理平台根据拆分请求中的拆分内容，产生多个随机数，随机数的数量和票据拆分目标产生的子票据的数量相同，分别对多个随机数和上述待拆分电子票据的ID哈希，生成多个待产生电子票据的编号，管理平台分别把上述随机数和对应产生的编号添加到拆分请求上，并使用平台私钥进行数字签名，生成拆分交易。

可选地，区块经过节点共识后被提交到区块链上存证，包括：

节点对拆分交易上的数字签名进行验证；其中，拆分交易在区块链网络上存证是指拆分交易所产生的电子票据信息和交易全流程的秘密存证。

可选地，获取所述区块链网络所返回的交易结果，包括：

发起组织的身份标识，上述拆分交易所拆分产生的新电子票据信息。

其中，所述区块链网络内共识上链的区块中所包含的交易信息和电子票据信息都是以密文形式存储的，管理平台在本地或者云端数据库是以明文形式存储所述交易信息和电子票据信息的。

第二方面，提供了一种基于区块链的电子票据查询方法，应用于管理平台，该方法包括：

获取组织发起的电子票据查询请求，对查询请求进行解析，获取查询请求发起组织的组织标识和查询内容；所述查询内容包括电子票据信息；

根据所述组织标识，获取管理平台中的组织权限信息；并对所述组织权限信息与所述查询请求中所需要的权限信息进行校验；

当所述组织权限信息与所述查询请求中的权限信息相匹配时，在管理平台中获取相应的电子票据信息；

将所获取的相应的电子票据信息向查询请求发起组织进行推送。

可选地，当所述组织权限信息与所述查询请求中的权限信息相匹配时，在管理平台中获取相应的电子票据信息，包括：

获取查询请求中的查询条件信息；通过查询请求中的组织标识确定组织身份；在管理平台中获取组织的权限信息，确定组织身份对应的权限是否可执行上述查询请求。

组织权限信息与查询请求中所需要的权限信息相匹配时，通过查询请求中的组织身份标识确定组织公钥；使用组织公钥对区块链网络中获取到的相应的电子票据信息进行加密处理，得到查询请求中的电子票据信息的加密信息。

可选地，该方法还包括：

所述组织权限信息与所述查询请求中所需要的权限信息不匹配时，向组织返回错误消息，即所述组织不具有上述电子票据信息的查询权限。

可选地，在管理平台中获取相应的电子票据信息，包括：

获取所述查询请求中的查询条件信息，所述查询条件信息包括至少一个目标维度的目标索引；根据所述至少一个目标维度的目标索引值，查询所述管理平台中的信息索引表，得到所述电子票据信息，其中，信息索引表包括已存储电子票据信息的组织标识以及不同维度的索引值。

可选地，将所获取的相应的电子票据信息向查询请求发起组织进行推送，包括：

将所获取的相应的电子票据信息向相应的组织进行推送，其中，电子票据信息为加密信息，组织使用加密使用的公钥对应的私钥进行解密获取到相应的电子票据信息的明文。

第三方面，提供了一种基于区块链的电子票据拆分装置，该装置包括：

获取模块，用于获取组织发起的电子票据拆分请求；

解析模块，用于对拆分请求进行解析，获取拆分请求发起组织的身份标识和拆分内容；

验证模块，用于对所述身份标识进行组织身份验证，同时对所述拆分内容进行合法性验证；

处理模块，用于在组织身份验证及合法性验证通过后，根据所述拆分请求生成拆分交易，并提交到区块链网络上；

传输模块，用于获取所述区块链网络所返回的交易结果；其中，所述交易结果是在区块链网络中通过将所述拆分交易经过节点验证打包到区块内，并经过节点共识后被提交到区块链上存证后得到。

第四方面，提供了一种基于区块链的电子票据查询装置，该查询包括：

获取模块，获取组织发起的电子票据查询请求，对查询请求进行解析，获取查询请求发起组织的组织标识和查询内容；所述查询内容包括电子票据信息；

校验模块，根据所述组织标识，获取管理平台中的组织权限信息；并对所述组织权限信息与所述查询请求中所需要的权限信息进行校验；

处理模块，当所述组织权限信息与所述查询请求中的权限信息相匹配时，在管理平台中获取相应的电子票据信息；

传输模块，将所获取的相应的电子票据信息向查询请求发起组织进行推送。

本申请实施例提供的技术方案通过发起电子票据拆分请求；对拆分请求进行解析，获取拆分请求发起组织的身份标识和拆分内容；对身份标识所对应的组织身份进行验证，同时对拆分内容的合法性进行验证；根据拆分请求生成拆分交易，并提交到区块链网络上；拆分交易经过节点验证被打包到区块内，区块经过节点共识后被提交到区块链上存证；向拆分请求的发起组织和供应链金融管理平台返回交易结果，可以看出，本申请管理平台将拆分交易和交易结果持久化存储，由此实现了将电子票据的灵活拆分，同时将电子票据信息和交易信息的哈希摘要在区块链网络中存证，保证了票据信息和交易信息的真实性和不可篡改性，公开可验证，同时存储于供应链金融管理平台中的票据信息和交易信息仅能够被权限相匹配的组织查询，保证了链上的隐私安全。

附图说明

为了更清楚地说明本发明的实施方式或现有技术中的技术方案，下面将对实施方式或现有技术描述中所需要使用的附图作简单地介绍。显而易见地，下面描述中的附图仅仅是示例性的，对于本领域普通技术人员来讲，在不付出创造性劳动的前提下，还可以根据提供的附图引申获得其它的实施附图。

图1是本发明实例提供的基于区块链技术的电子票据拆分方法的使用环境示意图；

图2是本发明实例提供的区块链网络200的功能架构示意图；

图3是本发明实例提供的电子设备的组成结构示意图；

图4为本发明实例提供的基于区块链技术的电子票据信息存储的一个数据结构图；

图5为本发明实例提供的基于区块链技术的交易信息存储的一个结构示意图；

图6为本发明实例提供的电子票据拆分的原理示意图；

图7为本发明实例提供的电子票据的内容示意图；

图8为本发明实例提供的基于区块链技术的电子票据拆分方法一个可选的流程示意图；

图9为本发明实例提供的电子票据信息及交易信息的数据查询方法一个可选的流程示意图；

图10为本发明实例提供的电子票据拆分的使用环境示意图。

具体实施方式

为了使本申请的目的、技术方案及优点更加清楚明白，以下结合附图及实施例，对本申请进行进一步详细说明。应当理解，此处描述的具体实施例仅仅用以解释本申请，并不用于限定本申请。

在本发明的描述中，术语“包括”、“具有”以及他们的任何变形，意图在于覆盖不排他的包含，例如，包括了一系列步骤或单元的过程、方法、系统、产品或设备不必限于已明确列出的那些步骤或单元，而是还可包含虽然并未明确列出的但对于这些过程、方法、产品或设备固有的其它步骤或单元，或者基于本发明构思进一步的优化方案所增加的步骤或单元。

对本发明的实施例进行进一步详细说明之前，对本发明实施例中涉及的名词和术语进行说明，本发明实例中涉及的名词和术语适用于如下的解释。

1）交易（Transaction），等同于计算机术语“事务”，交易包括了需要提交到区块链网络执行的操作，并非单指商业语境中的交易，鉴于在区块链技术中心约定俗成地使用了“交易”这一术语，本发明实施例遵循了这一习惯。

例如，部署（Deploy）交易用于向区块链网络中的节点安装指定的智能合约并准备好被调用；调用（Invoke）交易用于通过调用智能合约在区块链中追加交易的记录，并对区块链的状态数据库进行操作，包括更新操作（包括增加、删除和修改状态数据库中的键值对）和查询操作（即查询状态数据库中的键值对）。

2）电子票据，是由一家组织对另一家组织基于现实业务流转需要作出的付款承诺证明。

例如，组织A为组织B提供了某项服务，组织B应当向组织A付出相应报酬，但由于传统供应链中涉及到组织层级复杂，因此组织B所支付的报酬存在一定账期，无法直接立刻到达组织A。电子票据可看做组织B对组织A的一种付款承诺，其承诺由事先声明的担保人进行担保。

3）区块链（Blockchain），是由区块（Block）形成的加密的、链式的交易的存储结构。

例如，每个区块的头部既可以包括区块中所有交易的哈希值，同时也包含前一个区块中所有交易的哈希值，从而基于哈希值实现区块中交易的防篡改和防伪造；新产生的交易被填充到区块并经过区块链网络中节点的共识后，会被追加到区块链的尾部从而形成链式的增长。

4）区块链网络（Blockchain Network），通过共识的方式将新区块纳入区块链的一系列的节点的集合。

5）供应链金融（Service Chain of Finance），是指从供应链产业整体出发，运用金融科技手段，整合物流、资金流、信息流等信息，在真实交易背景下，构建供应链中占主导地位的核心企业与上下游企业一体化的金融供给体系和风险评估体系，从而降低企业成本，提升产业链价值。

6）共识（Consensus），是区块链网络中的一个过程，用于在涉及的多个节点之间对区块中的交易达成一致，达成一致的区块将被追加到区块链的尾部，实现共识的机制包括工作量证明（PoW，Proof of Work）、权益证明（Pos，Proof of Stake）、股份授权证明（DPos，Delegated Proof-of-Stake）、消逝时间量证明（PoET，Proof of Elapsed Time）等。

7）树列（TreeLink），树列是一组树的集合，但特别的是集合中所有树的根节点被放在一起组织成一个列表。通过树列的引入，为电子票据提供了灵活可拆分的性质，同时，大幅缩减了电子票据的查询时间。

8）哈希路径（Hash Path），哈希路径类似于上述区块链的性质描述，不同的是哈希路径更加简洁，通过对前一个数据量直接取哈希，得到新的数据量，如此循环，得到一个哈希路径。可选地，在取哈希时引入随机数，进一步增大哈希路径的安全空间。

例如，电子票据A被拆分成电子票据B和电子票据C，电子票据B和C的ID编号将通过哈希路径生成，即。



9）账本（Ledger），是区块链和与区块链同步的状态数据库的统称。其中，区块链是以文件系统中的文件的形式来记录交易；状态数据库是以不同类型的键值对的形式来记录区块链中的交易，用于支持对区块链中交易的快速查询。

10）智能合约（Smart Contracts），也称为链码（Chaincode）或应用代码，部署在区块链网络中的节点中的程序，节点执行接受的交易中所调用的智能合约，来对账本数据库的键值对对数据进行更新或查询的操作。

下面说明本发明实例提供的区块链网络的示例性应用，本申请中的管理平台可以是供应链金融管理平台，具体的请参见图1，图1是本发明实例提供的区块链中的基于区块链技术的电子票据拆分方法的使用环境示意图，包括区块链网络200（示例性示出了节点210-1至210-3）、供应链金融管理平台300、组织方400（示例性示出了归属于组织A节点系统400的终端410-1和410-2以及归属于组织B节点系统500的终端510-1），下面分别进行说明：

其中，区块链网络200的类型是灵活多样的，例如可以为公有链、私有链或联盟链中的任意一种。以公有链为例，任何业务主体的电子设备例如用户终端和服务器，都可以在不需要授权的情况下接入区块链网络200；以联盟链为例，业务主体在获得授权后其下辖的电子设备(例如终端/服务器)可以接入区块链网络200，此时，成为区块链网络200中的一类特殊的节点即客户端节点。

需要指出地，客户端节点可以只提供支持业务主体发起交易（例如，用于上链存储数据或查询链上数据功能），对于区块链网络200的常规节点210的功能，例如下文的排序功能、共识服务和账本功能等，客户端节点可以缺省或者有选择性（例如，取决于业务主体的具体也无需求）地实现。从而，可以将业务主体的数据和业务处理逻辑最大程度迁移到区块链网络200中，通过区块链网络200实现数据和业务处理过程的可信和可追溯。

区块链网络200接收来自不同业务主体的结点系统（例如图1中所示出的组织A节点系统400和组织B节点系统500）的客户端（例如，图1所示出的归属于组织A节点系统400的终端410-1和410-2以及归属于组织B节点系统500的终端510-1）提交的验证交易，执行交易以查询账本，并将查询结果返回给客户端。可以理解地，上文接收交易并执行交易的区块链网络200中的节点，具体是指区块链网络200中的原生节点210，当然，在业务主体的客户端具有区块链网络200中原生节点210的功能（例如共识功能、账本功能）时，也可以包括相应的客户端节点。

区块链网络200还接收来自供应链金融管理平台300提交的存证交易，执行交易以更新账本，并将更新结果返回给供应链金融管理平台和相应组织的客户端。

下面以多个业务主体（不同的机构节点系统）接入区块链以实现电子票据的可拆转融为例说明区块链技术的示例性应用。

参加图1，供应链环节涉及多个业务主体，如当前组织A节点系统400和组织B节点系统500，在获得供应链金融管理平台300的授权后，当前组织A节点系统400的终端410-1、410-2以及组织B节点系统的终端510-1都可以接入区块链网络200。

当前组织A节点系统400的业务人员在终端410-1上登录当前组织节点系统400，输入所要拆分电子票据的拆分请求或查询请求，其中，拆分请求被发送到供应链金融管理平台300，由供应链金融管理平台300根据所接收的拆分请求生成对应更新/查询操作的交易，在交易中指定了实现更新/查询操作需要调用的智能合约、以及向智能合约传递的参数，交易还携带了当前组织节点系统400签署的数字签名（例如，使用当前组织节点系统400的数字证书中的私钥，对交易的摘要进行加密得到）和供应链金融管理平台300签署的数字签名，并将交易广播到区块链网络200。

区块链网络中的节点210中接收到交易时，对交易携带的数字签名进行验证。验证成功后部署节点210自己的数字签名（例如，使用节点210-1的私钥对交易的摘要进行加密得到），并继续在区块链网络200中广播。

区块链网络200中具有排序功能的节点210接收到验证成功的交易后，将交易填充到新的区块中，并广播到区块链网络中200提供共识服务的节点。

下面说明本发明实例提供的区块链网络的示例性的功能架构，参加图2，图2是本发明实施例提供的区块链网络200的功能架构示意图，包括应用层、合约层、共识层、网络层和数据层，下面分别进行说明。

数据层封装了实现账本的各种数据结构，包括以文件系统中的文件实现的数据块，区块链的链结构，时间戳，加密用的哈希函数，交易存储的Merkle树及P2P用到的非对称加密。

网络层封装了点对点（P2P，Point to Point）网络协议、数据验证机制和业务主体身份管理的功能。

其中，P2P网络协议实现区块链网络200中节点210之间的通信，数据验证机制用基于密码学的方法（例如数字证书、数字签名、公私钥对）实现节点210之间传说数据的可靠性；主体身份管理功能用于根据实际的业务场景对加入区块链网络200的业务主体的身份进行认证，并在认证通过时赋予业务主体接入区块链网络200的权限；业务主体身份管理用于存储允许接入区块链网络200的业务主体的身份、以及权限。

共识层封装了区块链网络200中的节点210对区块达成一致性的机制（即共识算法）、账本管理和交易管理的功能。

共识算法包括POS、POW和PBFT算法，支持共识算法的可拔插性。

交易管理用于验证节点210接收到的交易中携带的数字签名，验证业务主体的身份信息，并根据身份信息判断其是否具有权限进行交易（从业务主体身份管理读取相关信息）；对于获得接入区块链网络200的授权的业务主体而言，均拥有认证中心颁布的数字证书，业务主体利用自己的数字证书中的私钥对提交的交易进行签名，从而生成自己的合法数字签名。

账本管理用于维护区块链和账本数据库。对于链上已完成共识的区块，追加到区块链的尾部；执行共识的区块中的交易，当交易包括更新操作时更新状态数据库中的键值对，当交易包括查询操作时查询账本数据库中的键值对并向业务主体返回查询结果。支持对账本数据库的多种维度的查询操作，包括：根据区块序列号(例如交易的哈希值)查询区块；根据区块哈希值查询区块；根据交易序列号查询区块；根据交易序列号查询交易；根据业务主体的账号(序列号)查询业务主体的账号数据；根据通道名称查询通道中的区块链。

合约层封装了区块链网络为实现各种业务所需的智能合约、链码和脚本代码。

应用层封装了区块链网咯能够实现的各种业务，包括票据拆分、账单查询和票据流转。

下面说明实现本发明实施例的区块链网络的节点的示例性结构，可以理解地，区块链网络200中任意类型的节点的硬件可以根据下文说明的硬件结构而实施。

下面对本发明实例提供的电子设备的组成结构做详细说明，其中，承载本发明所提供的基于区块链技术的电子票据拆分方法可以通过各类型电子设备来实施，如移动PC和专用服务器等。图3为本发明实施例提供的电子设备的组成结构示意图，可以理解，图3仅仅示出了电子设备的示例性结构而非全部结构，根据需要可以实施图3示出的部分结构或全部结构。

本发明实施例提供的电子设备包括：

信息传输模块，用于传输与组织身份相匹配的电子票据信息和交易信息；

信息验证模块，用于对组织身份信息进行验证，确定经过验证后的组织具有的交易权限；

信息验证模块，用于对交易进行验证，确定交易的合法性；

信息处理模块，用于通过组织的公钥对相关交易信息或电子票据信息进行加密，得到加密信息；

信息处理模块，用于基于组织标识、数据权限信息以及加密交易信息，电子票据信息，生成目标区块，并将目标区块加入到区块链网络中；

信息处理模块，用于基于上述加密信息，使用组织的私钥进行解密，得到交易信息或电子票据信息。

信息存储模块，用于基于上述交易信息、电子票据信息或加密信息进行持久化存储。

上述方案中，当其应用于供应链金融管理平台时：

信息传输模块，用于接收组织的电子票据拆分请求；

信息验证模块，用于响应于拆分请求，同时对拆分请求的发起组织进行身份验证；

信息验证模块，用于当发起组织的身份验证通过时，对拆分请求进行验证，确定拆分请求的合法性；

信息验证模块，用于当拆分请求合法时，生成拆分请求对应的拆分交易；

信息存储模块，用于对拆分交易进行持久化存储。

上述方案中，当其应用于区块链网络中时：

信息传输模块，用于接收供应链金融管理平台的拆分交易的存证请求；

信息验证模块，用于响应于相应存证请求，同时对供应链金融管理平台进行身份验证；

信息处理模块，用于当身份验证通过时，对存证请求进行解析，获得拆分交易；

信息处理模块，用于通过将拆分交易进行加密打包，得到加密信息；

信息存储模块，用于将加密信息持久化存储。

上述方案中，当其应用于区块链网络中时：

信息传输模块，用于接收组织的电子票据信息或交易信息的验证请求；

信息验证模块，用于验证验证请求的发起组织的身份信息；

信息处理模块，用于当身份验证通过时，对验证请求进行解析得到所要验证的电子票据或交易信息的ID标识；

信息处理模块，通过ID标识获取到对应的电子票据信息或交易信息的哈希摘要；

信息传输模块，将哈希摘要信息返回给验证请求的发起组织。

图4为本发明实例提供的基于区块链技术的电子票据信息存储的一个数据结构，树列（Treelink），可以理解地，图4所示的树列数据结构用来存储区块链网络内的电子票据信息。列表节点代表开始由发行组织最早发行的票据，每个列表结点对应一棵树用来存储电子票据的流转信息，例如可以是的电子票据经过一次拆分被拆分成和两张电子票据，可验证地，电子票据拆分前与拆分后的总价值不变，且拆分后的原票据将作废。电子票据流转的次数不受限制，且全部拆分过程都被记录在树列上。通过树列的引入，实现了电子票据的灵活拆分。

图5为本发明实例提供的基于区块链技术的交易信息存储的一个数据结构，默克尔树（Merkle Tree），可以理解地，图5所示的默克尔树用来存储区块链网络内的交易信息。默克尔树的底层节点是区块链网络收到的交易，对上述交易分别进行哈希加密，然后再以两个交易的哈希值作为输入，生成上层新的哈希值，层层递进，最后得到一个默克尔树根。默克尔树具有的特点是，底层的任何一笔交易发生篡改，都会影响默克尔树根值的变化,因此可以用来存储交易使其具有不可篡改性。

图6为本发明实例提供的电子票据拆分的原理示意图，可以理解地，本发明实施例中的电子票据拆分如图6所示，电子票据的主要字段包含1）ID（编号，即电子票据的身份标识，具有唯一性），2）FROM\_PATH（来源路径，即电子票据在树中所处的位置，例如单子票据的来源路径为，3）CURRENT\_OWNER（当前所有者，即电子票据现在的所有权归属），4）MNY（面值），5）R\_NUMBER（随机数，即为了使用哈希路径引入的参数）。另外，还有其他一系列其他属性在图示中未标出，可以理解地，实施例中仅展示出部分关键属性，但并不影响本发明提出的拆分方法的实施，具体的拆分原理如下：

例如，电子票据600-1的持有组织组织A提出拆分请求，通过验证后电子票据600-1在供应链金融管理平台上被拆分，拆分交易和拆分后产生的票据被保存在供应链金融管理平台上，同时供应链金融管理平台将拆分交易和拆分后产生的票据发送到区块链网络上加密存证。

其中，通过验证后在供应链金融管理平台上被拆分，通过验证是指对持有组织A的组织身份进行验证和对电子票据600-1的拆分合法性进行验证。被拆分是指供应链金融管理平台通过拆分请求构造拆分交易，产生拆分目标的新凭据，具体如下：生成和拆分目标相同数量的随机数（拆分目标是指票据拆分的目的，如票据600-1的拆分目的是拆分成MNY=1000和MNY=2000的两个票据，则拆分目标数量为2）；构造拆分交易，拆分交易在上述拆分请求的基础上添加随机数字段并由供应链金融管理平台签名；使用哈希函数计算上述拆分产生的电子票据（如);根据拆分请求中提供的参数生成新票据，参数包括拆分后新票据的归属权（CURRENT\_OWNER），来源路径（FROM\_PATH）等。至此，供应链金融管理平台根据上述拆分请求生成了对应的拆分交易和拆分目标产生的新票据，并对上述交易和票据进行签名。

图7为本发明实例提供的电子票据的内容示意图：其中，图示内容用于表示电子票据在不同流转阶段的电子票据信息，每一个电子票据信息均包括该票据在当前阶段的1）编号2）状态3）当前所有者4）金额5）来源路径6）到期时间7）随机数。由于传统技术中的电子票据信息采用中心化的存储方式，当前的电子票据信息一般只包含电子票据部分关键信息，无法全面覆盖所有信息。由于本发明采用供应链金融管理平台对上述电子票据信息进行明文存储，采用区块链网络对上述电子票据信息进行密文存证，组织通过向供应链金融管理平台提交交易请求进行交易，并通过向区块链网络发起数据查询请求验证账本的正确性，保证上述票据拆分在实现可灵活拆分的同时，可公开验证真实性和有效性，且不可篡改。

图8说明本发明实施例提供的信息处理方法，参加图8，图8为本发明实例提供的基于区块链技术的电子票据拆分方法的一个可选的流程示意图，可以理解地，图8所示的步骤可以由图3运行电子票据拆分交易的电子设备执行。下面针对图8的步骤进行说明：

步骤801：组织根据当前业务需求发起电子票据拆分请求；

其中，电子票据拆分请求包括拆分内容，发起组织身份标识，发起组织数字签名。拆分内容包含待拆分票据的标识，位置以及拆分目标（例如需要把面值为n的电子票据拆分成两张面值为n/2的电子票据，并分别把拆分产生的两张电子票据转让给其他组织A和B，则拆分目标为(）。发起组织身份标识是区块链网络内组织独一无二的身份证明，可选地，发起组织的身份标识可以设置为发起组织对应的公钥。发起组织数字签名代表了发起组织对该笔交易的许可，是由上述公钥对应的私钥生成的一串密码学字符串，供应链金融管理平台和区块链网络通过数字签名对组织的身份进行认证。

步骤802：供应链金融管理平台对上述拆分请求进行解析，获取拆分请求发起组织的身份标识和拆分内容。

步骤803：对上述身份标识所对应的组织身份进行验证，同时对上述拆分内容的合法性进行验证。

在本发明的一些实施例中，对组织的身份进行验证，确定经过验证的组织对上述拆分交易拥有所对应的交易权限，可以通过以下方式实现：

对上述组织的身份进行验证，当上述组织的身份标识与供应链金融管理平台中的原始数据相匹配时，确定经过验证上述组织为当前交易发起组织。通过上述组织的身份标识（实施例中直接令所属组织的身份标识为公钥，可选）对交易上附带的数字签名进行验证，确定经过验证的拆分交易请求是由组织提出的。上述两个条件必须同时满足，上述拆分请求的提出合法性才能被满足。

对上述拆分内容的合法性验证，包括对拆分内容中待拆分电子票据的存在性，有效期，所有权，是否双花以及等价值的验证，验证可以并行实施，故不会为系统带来额外的时间开销，具体验证方法如下：

对上述拆分内容的合法性进行验证，包括拆分内容中待拆分电子票据的存在性验证，待拆分电子票据的存在性验证可以通过待拆分电子票据的FROM\_PATH来完成。FROM\_PATH字段是待拆分电子票据在树列中的存储路径，通过FROM\_PATH的第一个字段，可以在供应链金融管理平台的数据库中所存储的数列列表中搜索，找到第一个字段对应的电子票据后，可根据后续FROM\_PATH的后续字段在上述电子票据对应的树中继续搜索，直至找到所要拆分的电子票据。若上述任何一步查找失败，则说明来源路径不合法或电子票据不存在，供应链金融管理平台向发起组织返回错误信息。

对上述拆分内容的合法性进行验证，包括拆分内容中电子票据的有效期进行验证，待拆分电子票据的有效期验证可以通过待拆分电子票据中的MATURITY\_TIME来完成。电子票据的有效期是指，电子票据在发行时由发行组织对其设立的生命周期，只有在生命周期内，发行组织才承认电子票据的有效性，反之，超出有效期之后，发行组织认为电子票据的有效性作废。电子票据的有效期验证可以通过待拆分电子票据中的MATRURITY\_TIME来完成，供应链金融管理平台通过读取当前时间和待拆分电子票据的有效期进行比较，若当前时间大于待拆分电子票据的有效期，则待拆分电子票据处于有效期内，反之，电子票据作废，供应链金融管理平台向发起组织返回错误信息。

对上述拆分内容的合法性进行验证，包括待拆分电子票据的所有权进行验证，待拆分电子票据的所有权验证可以通过CURRENT\_OWNER字段来完成。电子票据的所有权是指当前票据的受益组织，可以理解地，当前票据的受益组织是唯一可以对票据进行拆分操作的组织，可选地，其他组织可以对票据进行查询操作（其他组织可以是监管机构，风控机构等）。待拆分电子票据的所有权验证可以通过CURRENT\_OWNER字段来完成，供应链金融管理平台通过读取平台中保存的上述FROM\_PATH中描述的待拆分电子票据的原始数据的CURRENT\_OWNER字段，与当前交易发起组织的身份标识进行比较，若相匹配，则待拆分电子票据的所有权为当前交易发起组织所有，反之，组织无权对电子票据交易，供应链金融管理平台向发起组织返回错误信息。

对上述拆分内容的合法性进行验证，包括待拆分电子票据是否双花进行验证。双花是一种恶意的消费行为，本发明中特指已被花费的电子票据在一段时间后再次被重复发起交易，双花交易会对数字资产造成无法估计的损失。待拆分电子票据是否双花可以通过FROM\_PATH字段来验证，如上述待拆分电子票据的存在性验证方法，可以通过FROM\_PATH在供应链金融管理平台内找到待拆分电子票据的原始数据，并确定其在树列中的位置，根据树列的数据结构关系，通过验证上述位置后是否存在子节点即可验证电子票据是否已被花费，若电子票据已被花费，则上述位置一定会存在子节点。因此，若上述位置没有子节点，则待拆分电子票据尚未被花费，非双花，反之，待拆分电子票据已被花费，无法再次交易，供应链金融管理平台向发起组织返回错误信息。

对上述拆分内容的合法性进行验证，包括待拆分电子票据与拆分目标待产生的电子票据的等价值验证。等价值验证可以通过拆分内容中的拆分目标来进行验证，拆分目标是指，待拆分电子票据请求产生的新电子票据的价值组成（例如，3000—>2000&1000，表示价值3000单位的电子票据拆分成价值分别为2000和1000单位的新电子票据）。需要补充地是，拆分目标属于拆分请求和拆分交易中的内容，不包含与电子票据中，同时，拆分目标不指定新产生的电子票据的其他参数。待拆分电子票据与拆分目标待产生的电子票据的等价值验证可以通过拆分内容中的拆分目标来完成，若待拆分电子票据的价值与拆分目标待产生的电子票据的价值相等，则待拆分电子票据与拆分目标待产生的电子票据等价值，反之，则非等价值，供应链金融管理平台向发起组织返回错误信息。

步骤804：供应链金融管理平台根据上述拆分请求生成拆分交易。

其中，拆分交易是在拆分请求的基础之上进行构建的。供应链金融管理平台根据上述拆分请求中的拆分目标，产生多个随机数。随机数的数量和拆分目标中待产生的电子票据数量相同，分别对多个随机数和上述待拆分电子票据的ID哈希，生成多个待产生电子票据的编号。供应链金融管理平台分别把上述随机数和对应产生的编号添加到拆分请求上，并利用平台私钥进行数字签名。

步骤805：将拆分交易提交到区块链网络上。

其中，将拆分交易提交到区块链网络上的目的是将电子票据信息和交易全流程存证，打破了传统票据平台的中心化存储限制，组织可随时对区块链上存证的数据进行验证，同时，由于区块链网络上存储的均为加密数据，可接受验证但不会发生数据窃取，保护了供应链环节的隐私性。

步骤806：拆分交易经过节点验证后被打包到区块内，区块经过节点共识后被提交到区块链上。

其中，上述验证是指节点对拆分交易上的数字签名进行验证，不包含拆分交易的合法性验证。需要指出地，拆分交易上的数字签名为供应链金融管理平台的数字签名，而拆分请求上的数字签名为发起组织的数字签名。本步骤仅对供应链金融管理平台的数字签名进行验证，而不包含拆分交易的合法性验证，原因是通过供应链金融管理平台的数字签名，可以知道上述验证已经被供应链金融管理平台完成验证。这样设计简化了区块链网络的共识流程，可以有效提升区块链网络的吞吐量。

步骤807：返回交易结果。

其中，交易结果将由区块链网络返回给供应链金融管理平台和发起组织，包括：发起组织的身份标识，上述拆分交易所产生的新电子票据信息。

图9为本发明实例提供的电子票据信息及交易信息的数据查询方法一个可选的流程示意图：

步骤901：组织向供应链金融管理平台发起查询请求，并从区块链网络中获取所需查询信息的哈希摘要；

其中，组织可直接从区块链网络中获取需要查询内容的哈希密文。

步骤902：供应链金融管理平台接收查询请求，并解析查询请求以获得对应的组织标识和查询内容；

步骤903：根据组织标记，获取供应链金融管理平台中的组织权限信息；

步骤904：对组织权限信息与查询请求需要的权限信息进行校验；

可以理解地，供应链金融管理平台中存储的电子票据信息和交易信息属于隐私信息，不能直接提供给其他组织。故需要对组织的权限信息进行校验，校验的具体过程为：

通过查询请求中的组织标识确定组织身份；在供应链金融管理平台中获取所属组织权限信息的原始记录，确定上述组织身份对应的权限是否可执行上述查询请求。

步骤905：当组织权限信息与查询请求中的权限信息相匹配时，在供应链金融管理平台中获取相应的电子票据信息或交易信息。

其中，在供应链金融管理平台中获取相应的电子票据信息的方法为：获取查询请求中的查询条件信息，查询条件信息包括至少一个目标唯独的目标索引；根据至少一个目标维度的目标索引值，查询供应链金融管理平台中的信息索引表，得到电子票据信息或交易信息，其中，信息索引表包括已存储电子票据信息或交易信息的组织标识以及不同维度的索引值。

可以理解地，组织权限信息与查询请求中所需要的权限信息相匹配时，通过查询请求中的组织身份标识确定组织公钥；使用公钥对区块链网络中获取到的相应的电子票据信息进行加密处理，得到查询请求中的电子票据信息的加密信息。

组织权限信息与查询请求中所需要的权限信息不匹配时，向组织返回错误消息，即组织不具有上述电子票据信息的查询权限。

步骤906：响应于查询请求，将获取到的电子票据信息或交易信息向组织进行推送。

其中，组织收到上述电子票据信息或交易信息，但电子票据信息或交易信息是加密的，必须使用发起组织的私钥进行解密获取到相应的电子票据信息的明文，因此即使其他组织截取到上述加密信息，也无法获取到任何相关信息。

可以理解地，组织收到上述电子票据信息或交易信息后，通过私钥进行解密得到相应信息的明文，再对明文进行哈希加密与上述区块链网络中的哈希摘要进行比较，可验证上述供应链金融管理平台中的信息的真实性和有效性。

下面介绍本发明中，电子票据拆分、电子票据信息和交易信息查询的使用环境，参见图10，图10为本发明实例提供的电子票据拆分的使用环境示意图：其中，区块链网络中包括有基于区块链网络的组织A的客户端与对应的记账共识节点A，组织B的客户端与对应的共识记账节点B，核心组织的客户端与对应的记账共识节点C，金融机构的客户端与对应的观察节点D，监管部门的客户端与对应的观察节点E，其中，核心组织，组织A和组织B拥有对平台账本更新查询的操作权限，监管部门和金融机构拥有对平台账本查询的权限。

至此，对于电子票据拆分方法的实现，只有电子票据的当前所有者能进行操作；对于电子票据信息和交易信息查询方法的实现，有电子票据的当前所有者、核心企业、监管部门和金融机构能进行可选择性地操作。传统的票据系统，存在票据信息分散、票据保管难、开票手续繁琐等问题。当前的数字票据系统，由于数字信息的可复制性，会造成一系列假票、克隆票的鉴别困难问题。即使通过密码学技术可以对上述信息进行保护，但带来了较大的加解密开销，同时也无法实现灵活拆分，为数字票据的流通带来了较大阻碍。而基于区块链技术的电子票据拆分方法，在保证电子票据信息有效的前提下，支持灵活拆分，支持公开可验证，保护票据信息和交易信息的隐私性，只有指定权限的组织才能够对上述信息访问获取。由于链上对电子票据信息和交易信息真实性的保证，获取组织可以快速对待拆分电子票据进行核实和验证，这极大的促进了电子票据的发展。

本申请实施例还提供的一种基于区块链的电子票据拆分装置。装置包括：

信息获取模块，用于获取组织发起的电子票据拆分请求；

信息解析模块，用于对拆分请求进行解析，获取拆分请求发起组织的身份标识和拆分内容；

信息验证模块，用于对身份标识进行组织身份验证，同时对拆分内容进行合法性验证；

信息处理模块，用于在组织身份验证及合法性验证通过后，根据拆分请求生成拆分交易，并提交到区块链网络上；

信息传输模块，用于获取区块链网络所返回的交易结果；其中，交易结果是在区块链网络中通过将拆分交易经过节点验证打包到区块内，并经过节点共识后被提交到区块链上存证后得到。

本申请实施例还提供的一种基于区块链的电子票据查询装置。装置包括：

信息获取模块，获取组织发起的电子票据查询请求，对查询请求进行解析，获取查询请求发起组织的组织标识和查询内容；查询内容包括电子票据信息；

信息校验模块，根据组织标识，获取管理平台中的组织权限信息；并对组织权限信息与查询请求中所需要的权限信息进行校验；

信息处理模块，当组织权限信息与查询请求中的权限信息相匹配时，在管理平台中获取相应的电子票据信息；

信息传输模块，将所获取的相应的电子票据信息向查询请求发起组织进行推送。

本申请实施例提供的基于区块链的电子票据拆分装置用于实现上述基于区块链的电子票据拆分方法，关于基于区块链的电子票据拆分装置的具体限定可以参见上文中对于基于区块链的电子票据拆分方法的限定，在此不再赘述。上述基于区块链的电子票据拆分装置中的各个部分可全部或部分通过软件、硬件及其组合来实现。上述各模块可以硬件形式内嵌于或独立于设备中的处理器中，也可以以软件形式存储于设备中的存储器中，以便于处理器调用执行以上各个模块对应的操作。

以上所述实施例的各技术特征可以进行任意的组合，为使描述简洁，未对上述实施例中的各个技术特征所有可能的组合都进行描述，然而，只要这些技术特征的组合不存在矛盾，都应当认为是本说明书记载的范围。

以上所述实施例仅表达了本申请的几种实施方式，其描述较为具体和详细，但并不能因此而理解为对申请专利范围的限制。应当指出的是，对于本领域的普通技术人员来说，在不脱离本申请构思的前提下，还可以做出若干变形和改进，这些都属于本申请的保护范围。因此，本申请专利的保护范围应以所附权利要求为准。

说 明 书 附 图

GG221116182A

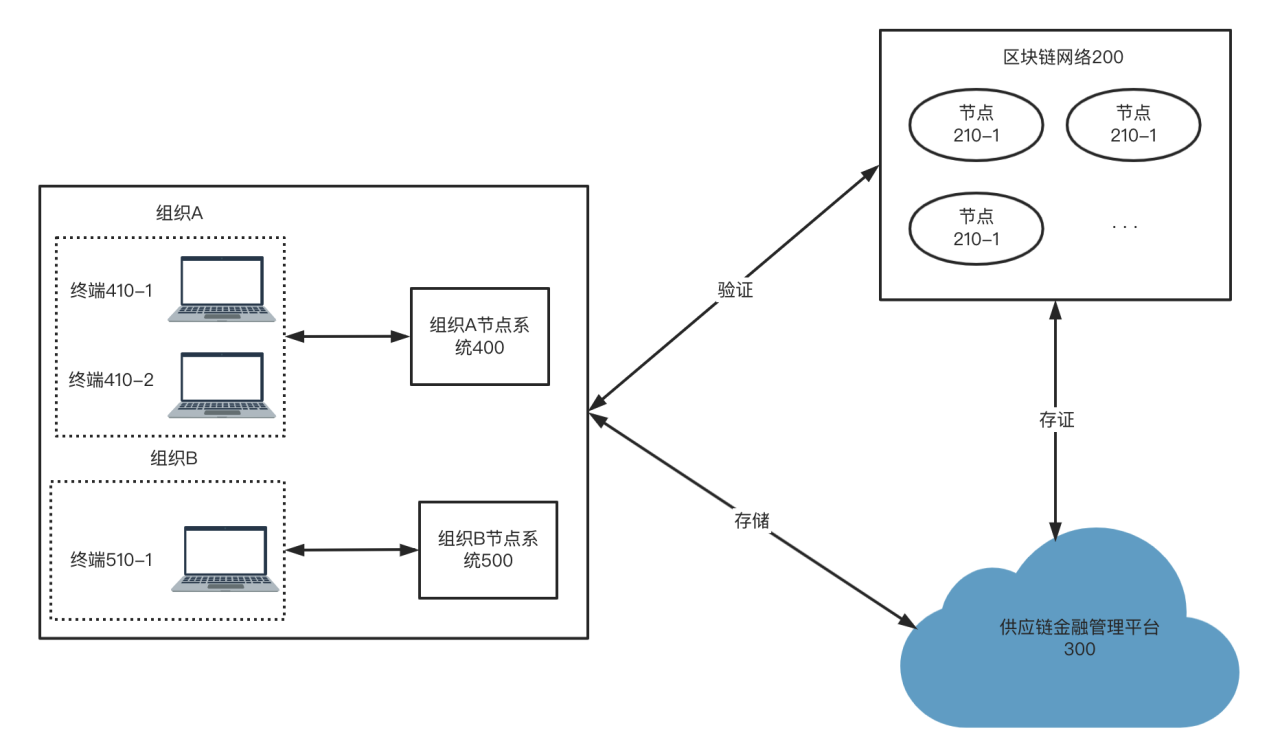
****

图1

****

图2

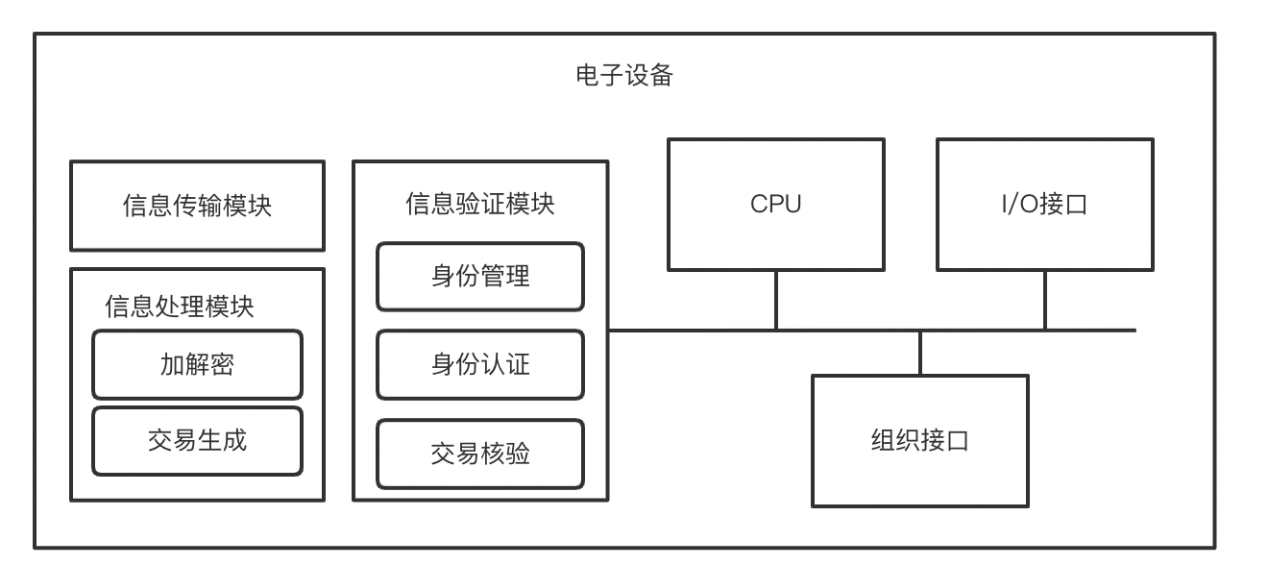
****

图3

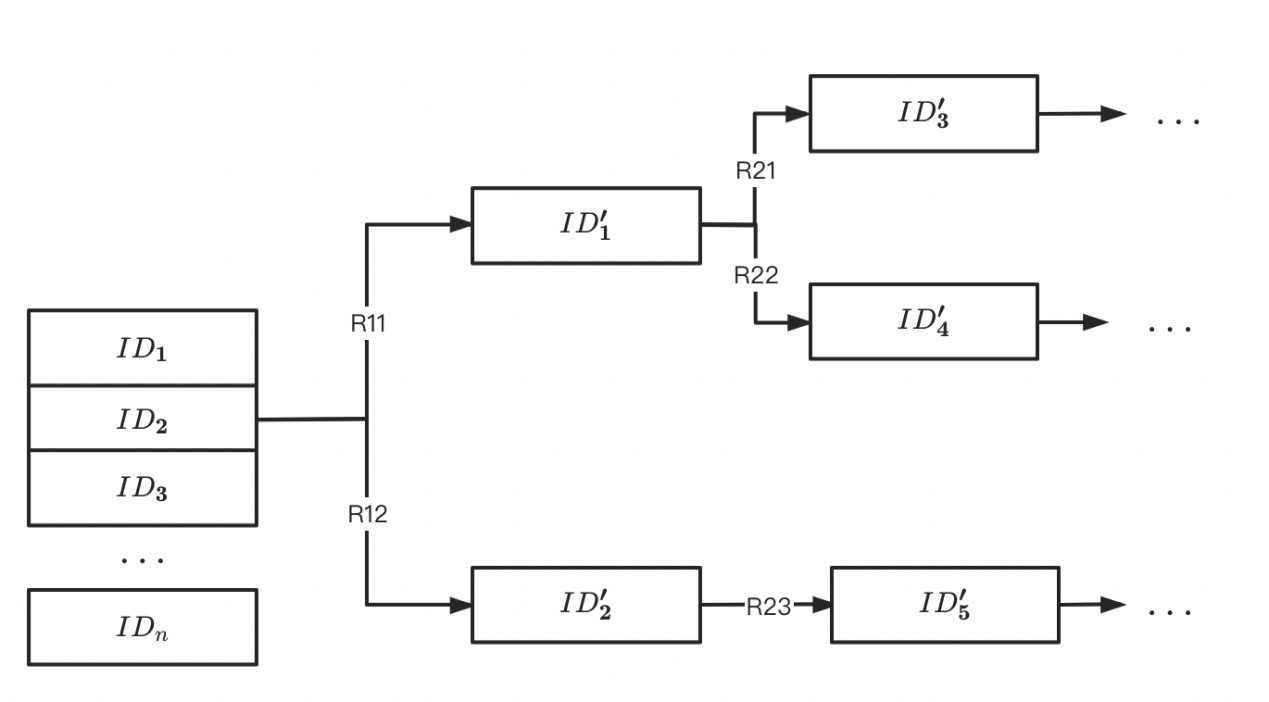
****

图4

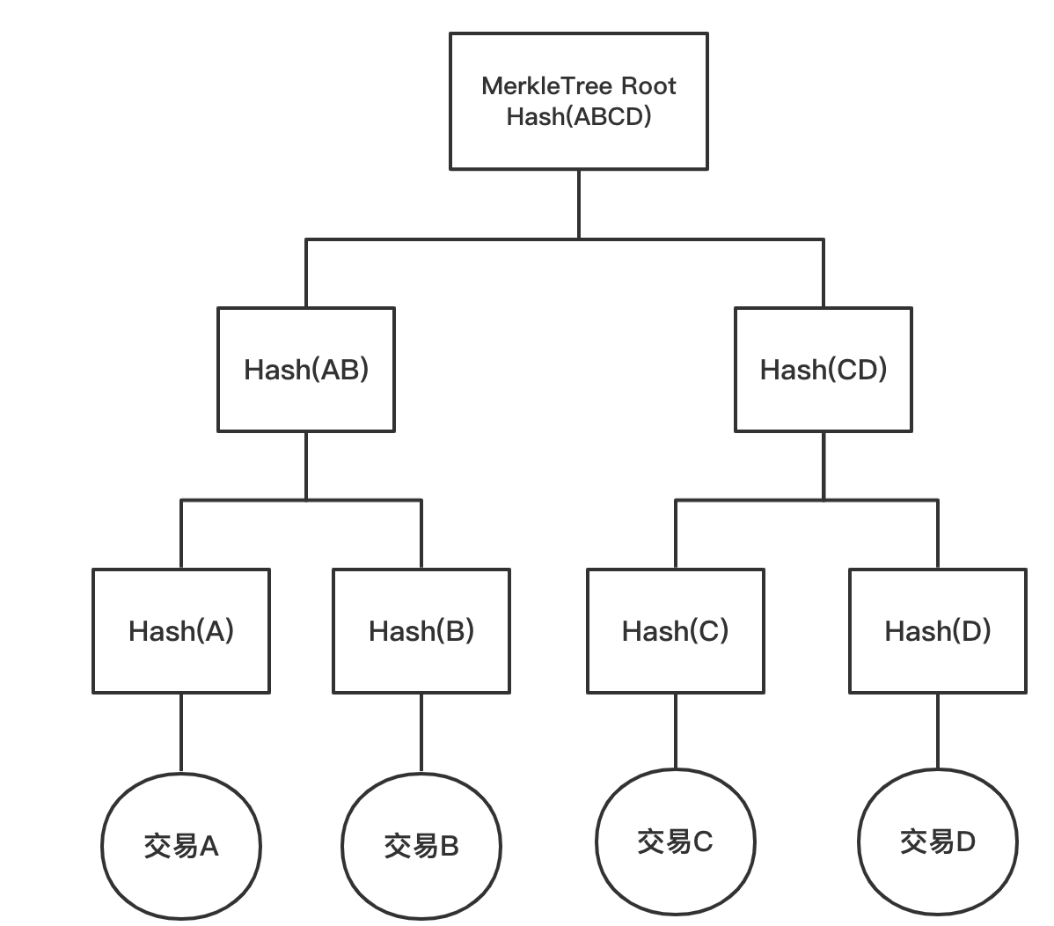
****

图5

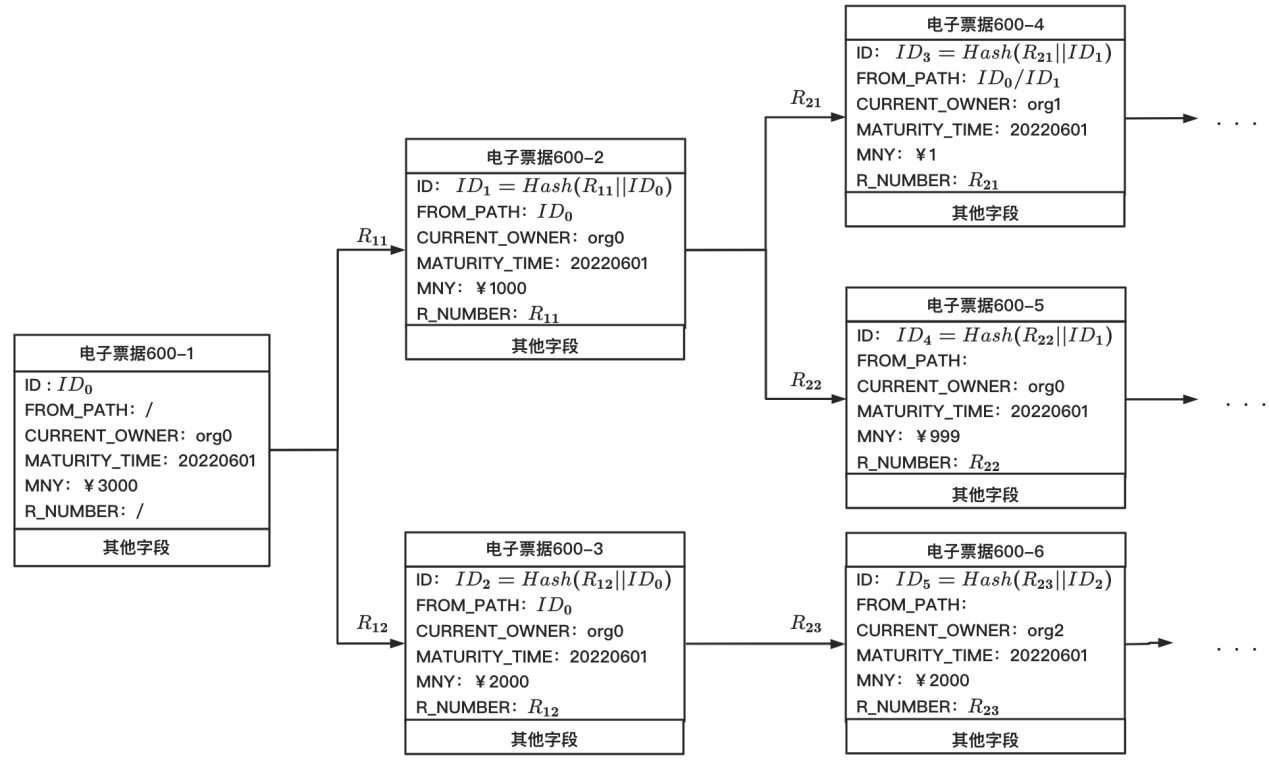
****

图6

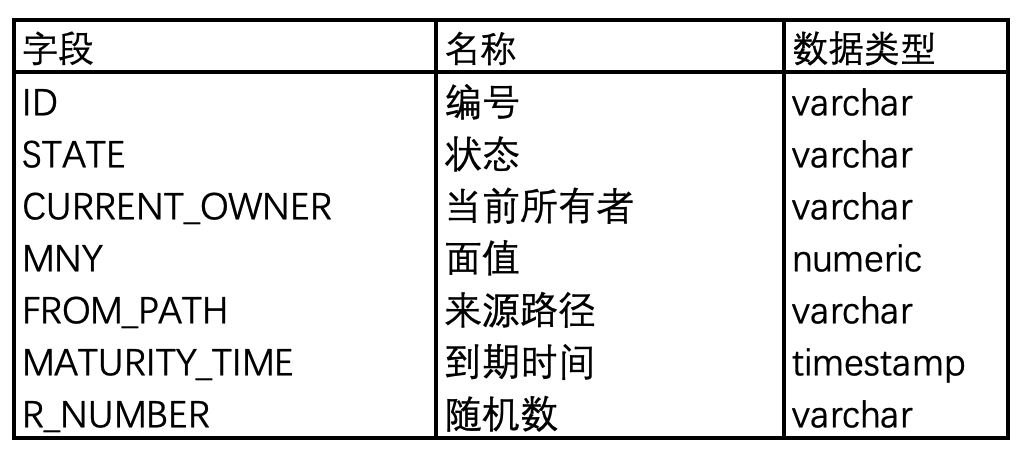
****

图7

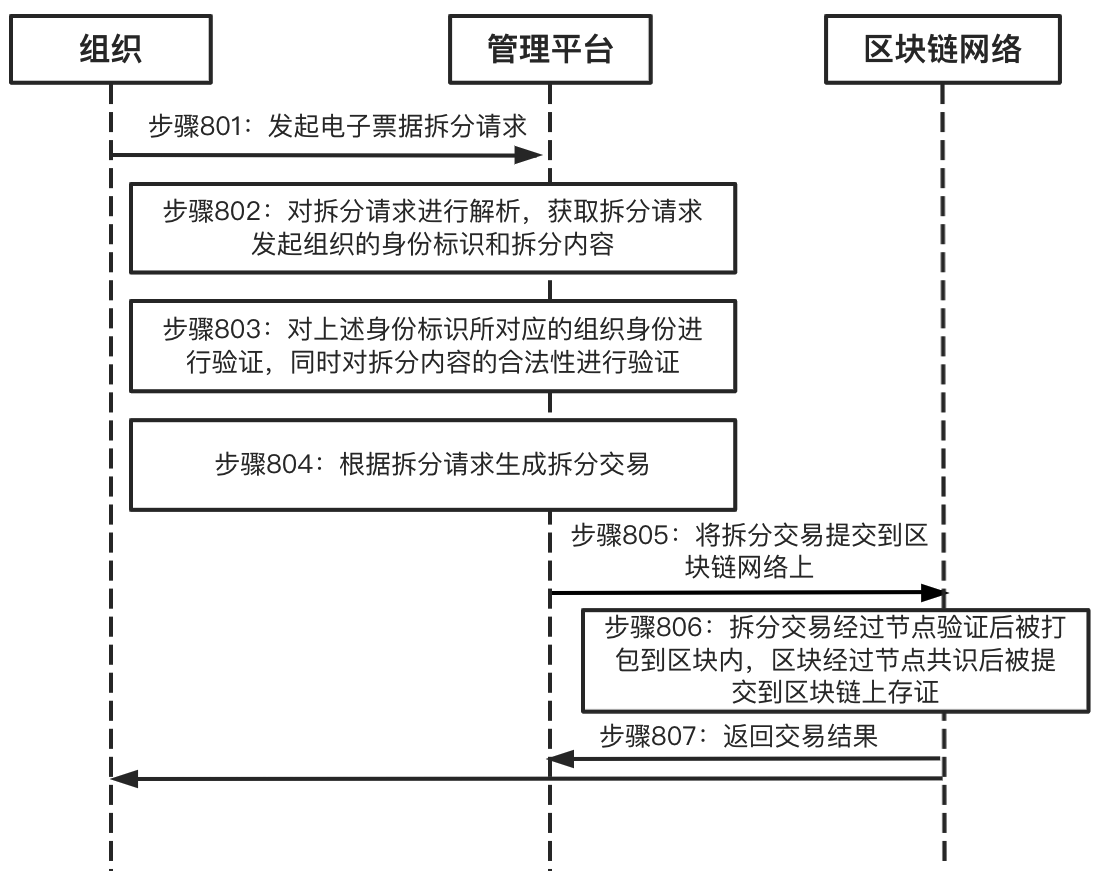
****

图8

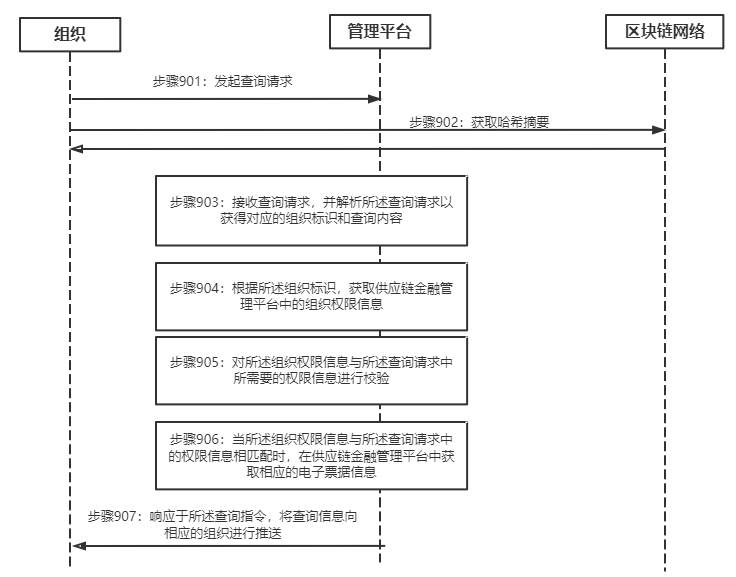
****

图9

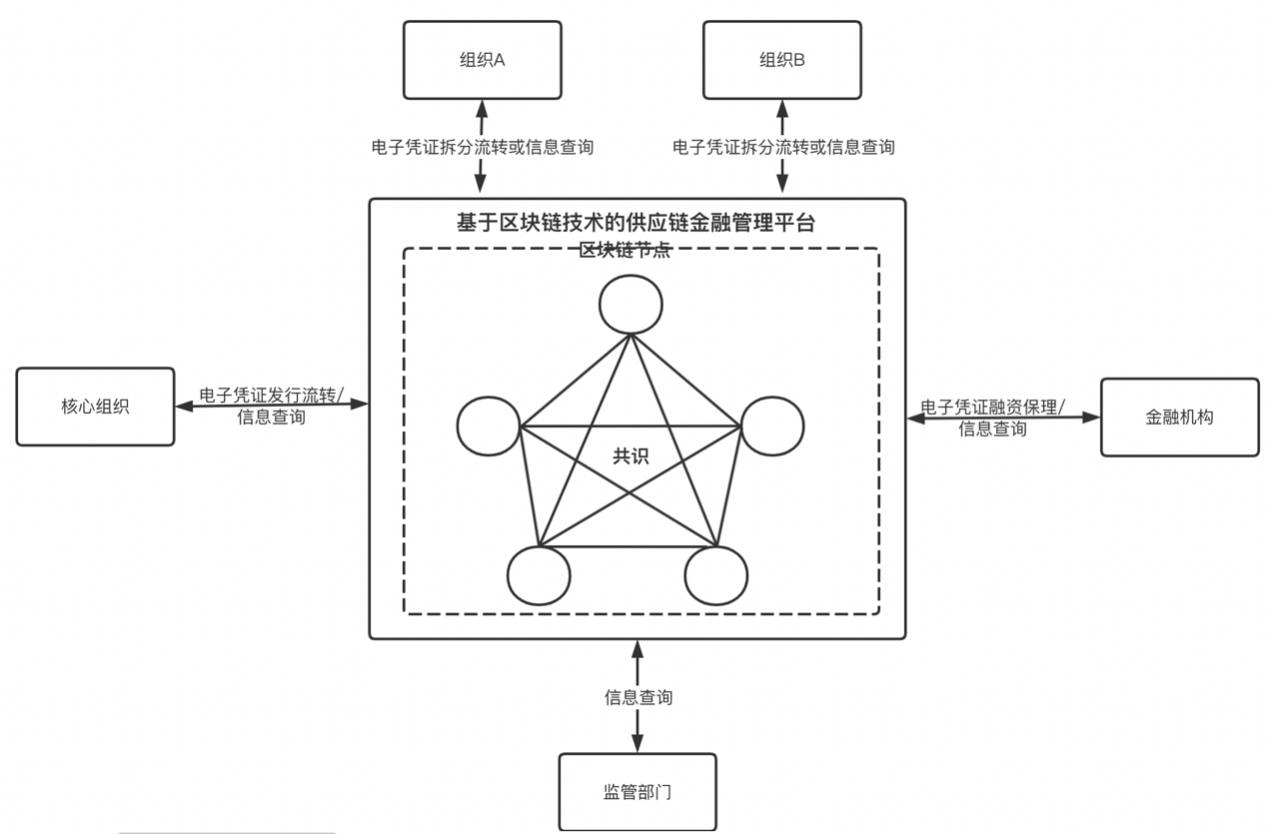
****

图10