(19)国家知识产权局

(12)发明专利

(10)授权公告号 CN 113014394 B
(45)授权公告日 2023.07.14

(21)申请号 202110196745.X

(22)申请日 2021.02.22

(65)同一申请的已公布的文献号
申请公布号 CN 113014394 A

(43)申请公布日 2021.06.22

(73)专利权人 北京工业大学
地址 100124 北京市朝阳区平乐园100号

(72)发明人 包振山 刘月 王凯旋 张文博

(74)专利代理机构 北京思海天达知识产权代理有限公司 11203
专利代理师 刘萍

(51)Int.Cl.
H04L 9/32(2006.01)
H04L 9/08(2006.01)
H04L 9/40(2022.01)
H04L 67/02(2022.01)

(56)对比文件
CN 109711836 A,2019.05.03
CN 110689433 A,2020.01.14
US 2019349199 A1,2019.11.14
周艺华等.基于区块链技术的数据存证管理系统.《技术研究》.2019,

审查员 黄菲

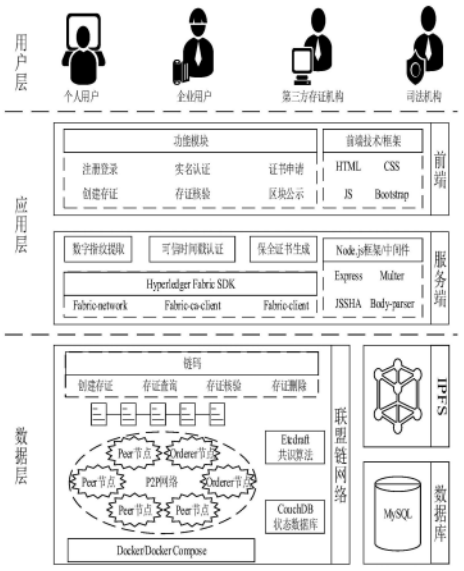
权利要求书2页 说明书5页 附图6页

(54)发明名称

基于联盟链的电子数据存证方法及系统

(57)摘要

本发明提供了一种基于联盟链的电子数据存证方法及系统，提出了基于分布式密钥生成协议的联盟链成员准入方法，底层联盟链不再依赖集中式CA节点，保证用户证书申请由用户独立完成，不需要第三方存证机构进行代理；提出了基于双密钥对机制和(t,n)门限加密算法的电子数据加解密方法，在确保用户所存证电子数据机密性的同时，保证司法机构可对电子数据真实性进行验证；提出了分散式的管理模式，避免了集中式管理模式带来的安全威胁。基于电子数据存证方法所实现的存证系统的系统架构，可分为用户层、应用层及数据层三层，包含注册登录、数据存证、数据核验、区块公示和个人中心五个模块。本发明能够保证电子数据存证安全可靠。



CN 113014394 B

1.基于联盟链的电子数据存证方法,其特征在于,包括:

一种基于分布式密钥生成协议的联盟链成员准入方法;用户证书的申请由用户独立完成;

一种基于双密钥对机制和(t,n)门限加密算法的电子数据加解密方法,n表示系统中司法节点总数,其中1<n;t表示其中部分司法节点;其中1≤t≤n;电子数据在传输或存储过程中进行加密处理,司法机构能够进行解密并对有效性进行验证;

无论是用户证书的颁发还是电子数据的解密均采用分散式的方式实现;

基于分布式密钥生成协议的联盟链成员准入方法,具体过程包括:

所有司法节点生成自签名证书,并将其发送给其它司法节点;

用户通过Web应用程序向系统发送一个包含其真实身份信息的证书请求;

所有司法节点验证用户身份信息的真实性,若验证未通过,则向用户发送一条拒绝消息,请求结束,若验证通过,所有司法节点共同执行分布式密钥生成协议,分布式密钥生成协议结束后,每个司法节点会获得一个相同的公钥(Public Key,PK)以及对应私钥(Secret Key,SK)的一个份额;

任选一个司法节点对包含用户的身份、公钥信息进行签名,并将生成的证书发送给Web应用程序;

所有司法节点将私钥份额及DKGP相关参数通过基于安全套接字层(Secure Sockets Layer,SSL)或安全传输层(Transport Layer Security,TLS)协议的安全通道发送给Web应用程序;

Web应用程序基于密钥份额和DKGP相关参数进行重构以获得完整的私钥,随后将证书及私钥存储到用户指定的本地目录中;

基于分布式密钥生成协议的密钥生成方法,具体过程包括:

系统中共有n个司法节点,用P_i表示,1≤i≤n,每个司法节点P_i随机选择两个参数,分别为p_i和q_i(p_i,q_i∈N*);

然后n个司法节点共同选定一个素数P′,满足P′>$\{n(3\times 2^{k-1})\}^2$,k是期望的密钥长度,1≤k;

通过BGW(M.Ben-Or,S.Goldwasser,and A.Wigderson)协议计算得到模数N和一个欧拉函数$\varphi(N)$,N是组成公钥的一个元素,$\varphi(N)$是私钥计算的构成部分;$N=\sum_{i=1}^{n}p_i\times\sum_{i=1}^{n}q_i \bmod P'$,mod是求余函数,$\varphi(N)=N+1-\sum_{i=1}^{n}(p_i+q_i)$;

所有司法节点协同执行分布式测试,以确保模数N是两个素数的乘积,即N=a×b,a、b是两个素数;

当能确保模数N是两个素数的乘积,则每个司法节点P_i随机地选择两个整数,分别用β_i和R_i表示,其中$\beta_i\in[0,10^4N]$,$R_i\in[0,10^8N]$,1≤i≤n;

所有司法节点发布一个多项式θ‘,θ‘是组成公钥的一个元素,通过BGW协议计算而得,$\theta'=n!\,\varphi(N)(\sum_{i=1}^{n}\beta_i)+N\sum_{i-1}^{n}n!\,R_i$;

公钥PK=(N,N+1,θ′),私钥$SK=n!\,\varphi(N)(\sum_{i=1}^{n}\beta_i)$;

基于双密钥对机制和(t,n)门限加密算法的电子数据加解密方法,具体过程包括:

用户请求入网时,所有司法节点连续执行两次DKGP以分别生成用于签名和加密的公私钥对,司法节点对加密用途私钥的份额进行备份;

通过Web应用程序,用户使用加密用途的公钥对所需存证的电子数据进行加密,并使用签名用途的私钥对包含电子数据密文的事务请求进行签名后,将事务请求提交到系统;

n个司法节点中的t个节点使用其备份的私钥份额共同解密电子数据密文,并对电子数据源数据的真实性进行验证;

若验证未通过,则向用户发送一条失败消息,若验证通过,则将电子数据的哈希值以及包括数据名称、格式、大小这些数据的元数据进行上链固化。

2.根据权利要求1所述的基于联盟链的电子数据存证方法,其特征在于:.

多个司法节点共同扮演CA(Certificate Authority)角色,即使部分节点受到攻击,攻击者也不能轻易地把自己注册成合法用户,从而获得底层联盟链的访问权限;

借助于(t,n)门限加密算法,至少需要n个司法节点中t个的私钥份额才能恢复原始数据;即使遭受攻击,只要攻击者掌控的司法节点数量不超过t个,用户的数据依旧是安全的;此外,多个司法节点还共同发挥着密钥管理中心的作用。

基于联盟链的电子数据存证方法及系统

技术领域

[0001] 本发明涉及区块链技术领域，尤其涉及一种基于联盟链的电子数据存证方法及系统。

背景技术

[0002] 随着信息技术的迅速发展，司法领域的证据种类不断进行扩充与完善。电子合约、电子票据、网页截图、电话录音等电子数据都已成为新型的电子证据材料，而普通电子数据具有易拷贝、易篡改、不易保存、证明力低等特点，所以通常不受司法认可。电子数据存证系统能够为电子数据的取证、存证及用证提供全链路服务，从而进一步提高了电子数据的公信力。

[0003] 现有的大多数存证系统依旧采用的是中心化的系统架构，时刻面临着系统崩溃、遭受攻击、人为篡改等固有风险，可能会发生数据丢失、数据泄露、数据篡改等严重的信息安全事故。区块链技术的分布式存储、不可篡改及可追溯等特性为电子数据存证提供了新的解决方案。部分司法机构联合第三方存证机构基于联盟链共同建立多中心的电子数据存证系统，从而保证了电子数据的完整性，避免了中心化系统架构带来的安全问题。由于电子数据保全的专业性，司法机构不得不引入第三方存证机构以寻求技术支持并将其作为合法的电子数据保全主体，所以存证系统的对外服务以及底层联盟链的部署与维护均由第三方存证机构所主导。但与此同时，在基于联盟链的存证系统中引入第三方存证机构将导致用户对系统产生根本性的信任问题。第三方存证机构可能引发的安全问题如下：

[0004] 1.第三方存证机构非法冒充平台用户创建存证。现有存证系统的使用过程中，用户注册登录并完成实名认证后，便可开始创建存证，而用于与底层联盟链交互的数字身份由第三方存证机构代替用户向证书颁发机构(Certificate Authority,CA)申请。因此，用户数字身份的管理权与使用权完全由第三方存证机构掌握，第三方存证机构可随意冒充用户创建存证。由于签名具有不可抵赖性，平台用户极有可能因此而承担额外的法律责任。

[0005] 2.用户所存证电子数据的机密性无法得到保证。现有存证系统的使用过程中，第三方存证机构会将用户所提交的电子数据存储在其本地数据库中以供用户自身访问或司法机构调用，但第三方存证机构可能会泄露用户的电子数据以牟利，这将严重损害用户的权益。

[0006] 3.用户所存证电子数据的真实性无法得到保证。第三方存证机构进行存证前并不对电子数据的真实性作任何验证。联盟链仅仅能够确保数据上链后无法被篡改，但无法确定上链前是否真实可信，所以存证系统可能会存储大量无效的电子数据。此外，电子数据的时效性较强，若等到发生纠纷时再验证其真实性，成本过高，并且结果可能不准确。

[0007] 因此，现有的基于联盟链的电子数据存证系统解决了电子数据的完整性问题，但平台用户的权益以及电子数据的真实性没有得到有效保障。

发明内容

[0008] 本发明旨在提供一种更安全的电子数据存证方案,以解决现有基于联盟链的存证系统所存在的不足。首先,用户证书的申请应由用户独立完成,而不需要第三方存证机构进行代理,并且底层联盟链不应依赖于集中式的CA节点。其次,电子数据在传输或存储过程中均需要进行加密处理,但同时需要保证司法机构能够进行解密并对有效性进行验证。最后,无论是用户证书的颁发还是电子数据的解密均需要采用分散式的方式来实现,从而避免集中式管理模式带来的安全威胁。

[0009] 为实现上述目的,本发明一方面提供了一种基于分布式密钥生成协议(Distributed Key Generation Protocol,DKGP)的联盟链成员准入方法,具体过程包括:

[0010] 所有司法节点生成自签名证书,并将其发送给其它司法节点;

[0011] 用户通过Web应用程序向系统发送一个包含其真实身份信息的证书请求;

[0012] 所有司法节点验证用户身份信息的真实性,若验证未通过,则向用户发送一条拒绝消息,请求结束,若验证通过,所有司法节点共同执行DKGP,协议结束后,每个司法节点会获得一个相同的公钥以及对应私钥的一个份额;

[0013] 任选一个司法节点对用户的身份、公钥等信息进行签名,并将生成的X.509证书发送给Web应用程序;

[0014] 所有司法节点将私钥份额及DKGP相关参数通过基于SSL或TLS协议的安全通道发送给Web应用程序;

[0015] Web应用程序基于密钥份额和DKGP相关参数进行重构以获得完整的私钥,随后将证书及私钥存储到用户指定的本地目录中。

[0016] 其中,基于分布式密钥生成协议的密钥生成方法,具体过程包括:

[0017] 每个司法节点P_i(1≤i≤n)随机选择两个参数p_i及q_i,然后共同选定一个大素数$P'>\{n(3\times 2^{k-1})\}^2$,k是期望的密钥长度。

[0018] 通过计算得到$N=\sum_{i=1}^{n}p_i\times\sum_{i=1}^{n}q_i\ modP'$。每个节点在这一步结束后共享一个多项式$\varphi(N)=N+1-\sum_{i=1}^{n}(p_i+q_i)$。

[0019] 所有司法节点协同执行分布式测试,以确保N=a×b,a,b是两个素数。若没有符合要求的a,b,则重复以上内容。

[0020] 若能确保N是两个素数的乘积,则每个司法节点P_i随机地选择两个整数$\beta_i\in[0,MN]$与$R_i\in[0,M^2N]$,M是足够大的正整数,以至于1/M的大小是可忽略的。

[0021] 所有司法节点计算并发布$\theta'=\Delta\varphi(N)(\sum_{i=1}^{n}\beta_i)+N\sum_{i-1}^{n}\Delta R_i$,Δ=n!。公钥PK=(N,G,θ′),其中G=N+1。私钥$SK=\Delta\varphi(N)(\sum_{i=1}^{n}\beta_i)$。

[0022] 另一方面,本发明提供了一种基于双密钥对机制和(t,n)门限加密算法的电子数据加解密方法,该方法既能够保证用户所存证电子数据的机密性,又能够保证司法机构可对电子数据的真实性进行验证,具体过程包括:

[0023] 用户请求入网时,所有司法节点连续执行两次DKGP以分别生成用于签名和加密的公私钥对,司法节点对加密用途私钥的份额进行备份;

[0024] 通过Web应用程序,用户使用加密用途的公钥对所需存证的电子数据进行加密,并

使用签名用途的私钥对包含电子数据密文的事务请求进行签名后，将事务请求提交到系统；

[0025] n个司法节点中的t个节点使用其备份的私钥份额共同解密电子数据密文，并对电子数据源数据的真实性进行验证；

[0026] 若验证未通过，则向用户发送一条失败消息，若验证通过，则将电子数据的哈希值以及数据名称、格式、大小等元数据进行上链固化。

[0027] 本发明与现有的基于联盟链的电子数据存证系统最大的不同在于采用了分散式的管理模式，因而具有更高的安全性，主要体现在如下两个方面：

[0028] 1.多个司法节点共同扮演着CA的角色，即使部分节点受到攻击，攻击者也不能轻易地把自己注册成合法用户，从而获得底层联盟链的访问权限。通过这种方法，有效地克服了集中式CA的脆弱性。

[0029] 2.借助于(t,n)门限加密算法，至少需要n个监管者中的t个监管者的私钥份额才能恢复原始数据。即使遭受攻击，只要攻击者掌控的司法节点数量不超过t个，用户的数据依旧是安全的。此外，多个司法节点还共同发挥着密钥管理中心的作用，有效地避免了因私钥丢失而造成的数据无法恢复的问题。

附图说明

[0030] 图1为电子数据存证系统的系统架构图。

[0031] 图2为Fabric联盟链网络的节点结构图。

[0032] 图3为系统注册登录模块流程图。

[0033] 图4为系统实名认证和证书请求模块流程图。

[0034] 图5为系统创建存证模块流程图。

[0035] 图6为系统存证核验模块流程图。

具体实施方式

[0036] 为使本领域技术人员更好地理解本说明书实施例中的技术方案，下面将结合本说明书实施例中的附图，对本说明书实施例中的技术方案进行详细地描述。显然，所描述的实施例仅是本说明书的一部分实施例，而不是全部的实施例。基于本说明书中的实施例，本领域普通技术人员所获得的所有其他实施例，都包含在本发明的保护范围之内。

[0037] 图1描述了基于所提出的电子数据存证方法所实现的存证系统的系统架构，自上及下可分为用户层、应用层及数据层三个层次。

[0038] 所述用户层包括个人用户、企业用户、第三方存证机构以及司法机构。个人用户和企业用户是具有存证需求的存证主体，也是系统的主要使用者，第三方存证机构的用户主要是负责系统应用层管理与维护工作的技术人员，而司法机构的用户则主要是在电子数据进行上链固化之前对其真实性进行验证的检验人员。

[0039] 所述应用层包括Web前端和Node.js服务端。前端使用HTML、CSS、JS、Bootstrap开发框架以及Ajax异步请求等技术实现系统的界面展示以及行为交互。服务端采用Express框架与Multer、Body-parser等中间件为前端提供特定的服务，并基于相应的SDK访问所述数据层，进行数据的读取或更新。

[0040] 所述数据层包括IPFS分布式文件系统、MySQL关系数据库以及Fabric联盟链。IPFS用于存储加密的电子数据，防止数据发生丢失。MySQL用于存储用户的账号、密码等基本数据，还可用于缓存IPFS中存储的电子数据，从而提高检索速度。Fabric联盟链则用于固化用户所存证电子数据的相关信息。

[0041] 本实施例中的Fabric联盟链由互联网法院、仲裁委员会、公证处、司法鉴定中心及第三方存证机构五个组织共同建立。图2描述了Fabric联盟链网络的节点结构，每个组织均包含三个Peer节点和三个CouchDB状态数据库节点，并且Peer0作为组织的锚节点。排序服务由六个Orderer节点提供，并采用Etcdraft共识算法。基于Docker/Docker Compose容器技术，这些节点可部署在局域网/广域网环境下的任何满足性能需求的服务器、主机或终端设备上。

[0042] 本实施例中的Web应用程序主要为所述个人用户、企业用户提供注册登录、实名认证、证书申请、创建存证、存证核验、区块公示等功能模块。

[0043] 图3描述了所述注册登录模块的流程图。用户首次访问系统时，需要注册账号并进行登录，具体步骤如下：

[0044] 个人用户在注册界面的表单中输入邮箱及密码，而企业用户则需要额外提供企业名称及企业代码，随后点击注册；

[0045] Web前端自动校验输入内容的格式是否正确，随后向Node.js服务端提交注册请求；

[0046] 注册完成后，引导用户进入登录界面，用户在表单中输入邮箱及密码，随后点击登录；

[0047] Web前端自动校验输入邮箱的格式是否正确，随后向Node.js服务端提交登录请求；

[0048] Node.js服务端检索MySQL数据库中是否存在与之相匹配的账户，若存在，则跳转到首页，否则提示用户登录失败。

[0049] 图4描述了所述实名认证和证书申请模块的流程图。用户注册并登录后，在存证电子数据之前，还需要完成实名认证并申请证书，具体步骤如下：

[0050] 用户在实名认证界面的表单中输入姓名和身份证号并点击认证；

[0051] Node.js服务端对其实名信息进行验证，若验证通过，则将实名信息记录到MySQL数据库和Fabric联盟链中，实名认证完成；

[0052] 用户在证书申请界面点击申请，司法节点收到请求后，共同执行两次DKGP，将生成的证书、私钥份额及DKGP相关参数发送到Web前端，并对加密用途私钥的份额进行备份；

[0053] Web前端基于密钥份额和DKGP相关参数进行重构以获得完整的私钥，随后将证书及私钥存储到用户指定的本地目录中，证书请求完成。

[0054] 图5描述了所述创建存证模块的流程图。用户拥有用于签名与加密的证书及私钥后，便可存证电子数据，系统能够存证的电子数据类型包括文件与文本，具体步骤如下：

[0055] 用户在创建存证界面选择文件或输入文本并填写名称及备注信息后，点击提交；

[0056] Web前端提取电子数据的数字指纹，并利用本地AES密钥对电子数据进行加密，同时使用用户加密用途的公钥对AES密钥执行加密操作，随后使用签名用途的私钥对包含电子数据指纹、电子数据密文及AES密钥密文的请求进行签名后，将其提交给系统；

[0057] Node.js服务端将电子数据密文存储到IPFS中，所有司法节点则使用其备份的私钥份额共同解密AES密钥密文，然后使用获得的AES密钥解密电子数据并对其真实性进行验证，若验证通过，则将数据明文哈希、数据密文哈希、AES密钥密文以及数据名称、数据备注、数据格式、数据大小、数据所有者等元数据打包成事务区块并提交到Fabric联盟链进行上链固化，否则提示用户数据存证失败。

[0058] 图6描述了所述存证核验模块的流程图。电子数据存证完成后，用户则可通过存证编码或数据哈希进行数据核验，以判断Fabric联盟链中是否已固化目标存证数据，具体步骤如下：

[0059] 用户在存证核验界面选择核验方式并输入核验内容后，点击核验；

[0060] Node.js服务端通过SDK检索Fabric联盟链中存证的电子数据，若存在目标存证记录，则将核验结果发送到Web前端，否则提示用户核验失败。

[0061] 所述区块公示模块用于向用户展示Fabric联盟链的区块信息。用户不仅可以在区块公示界面查看Fabric联盟链当前的区块高度以及任意区块的区块编号、数据哈希、成块时间及事务数量等信息，还能够通过存证事务所属区块的哈希字符串检索目标区块。

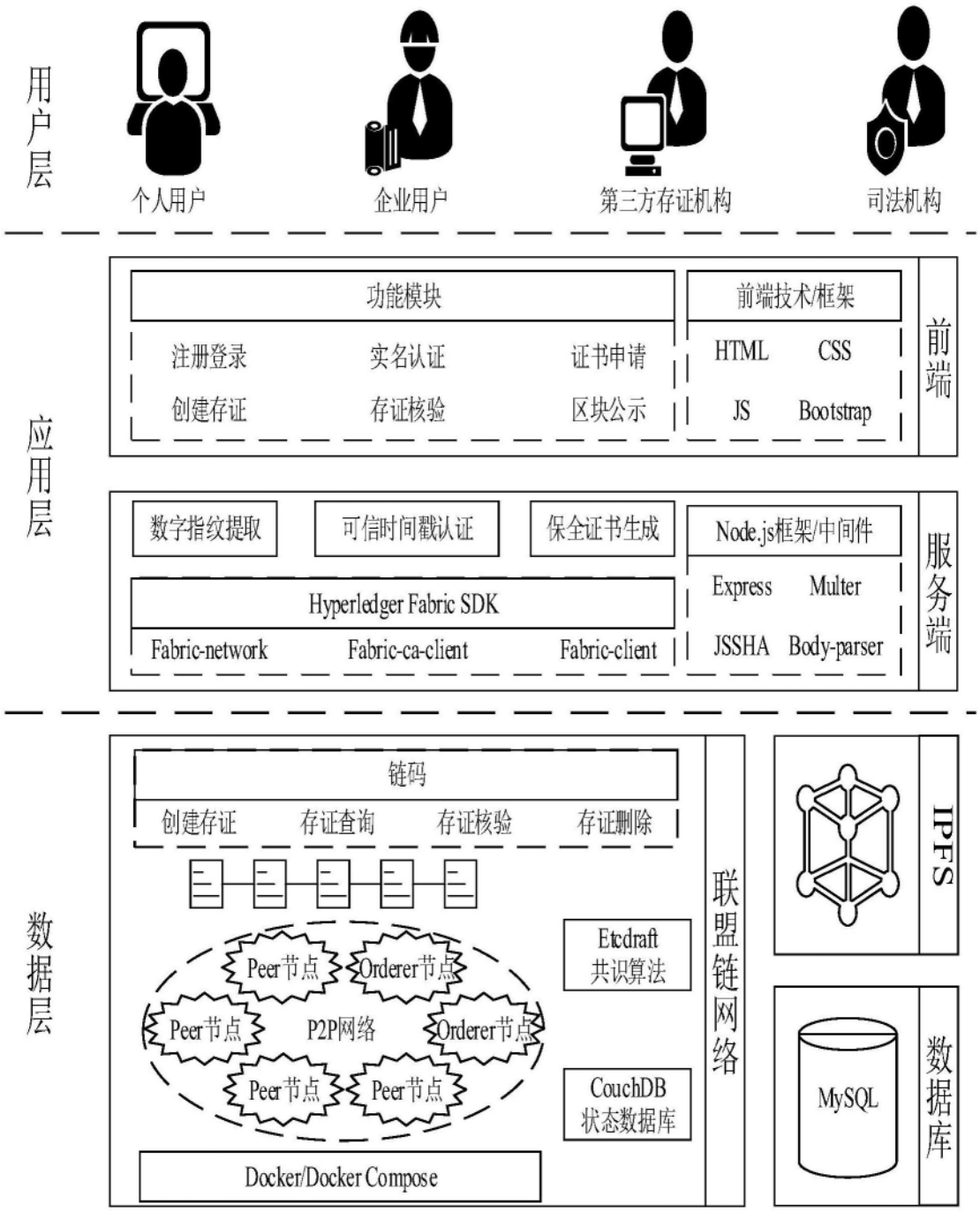

用户层
个人用户
企业用户
第三方存证机构
司法机构
应用层
功能模块
注册登录
实名认证
证书申请
创建存证
存证核验
区块公示
前端技术/框架
HTML
CSS
JS
Bootstrap
前端
数字指纹提取
可信时间戳认证
保全证书生成
Hyperledger Fabric SDK
Fabric-network
Fabric-ca-client
Fabric-client
Node.js框架/中间件
Express
Multer
JSSHA
Body-parser
服务端
数据层
链码
创建存证
存证查询
存证核验
存证删除
Peer节点
Orderer节点
Peer节点
P2P网络
Orderer节点
Peer节点
Peer节点
Etcdraft
共识算法
CouchDB
状态数据库
Docker/Docker Compose
联盟链网络
IPFS
MySQL
数据库

图1

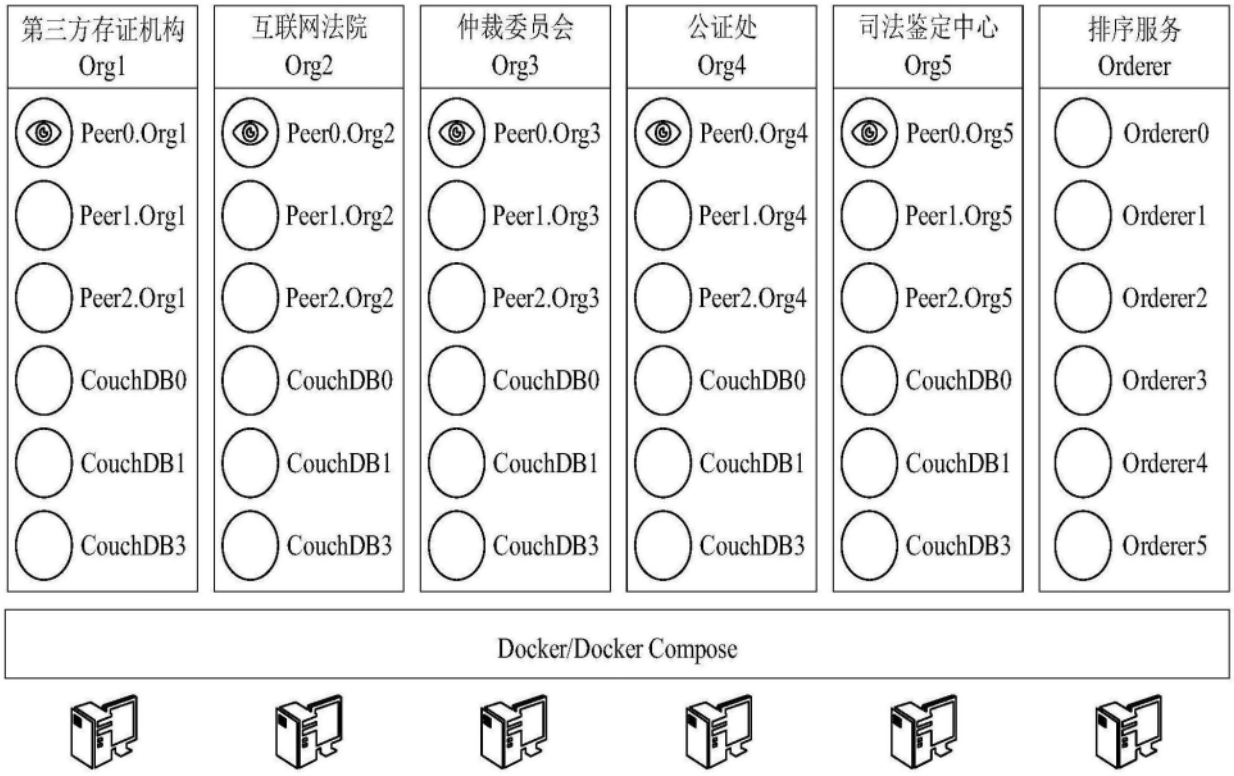

第三方存证机构
Org1
Peer0.Org1
Peer1.Org1
Peer2.Org1
CouchDB0
CouchDB1
CouchDB3
互联网法院
Org2
Peer0.Org2
Peer1.Org2
Peer2.Org2
CouchDB0
CouchDB1
CouchDB3
仲裁委员会
Org3
Peer0.Org3
Peer1.Org3
Peer2.Org3
CouchDB0
CouchDB1
CouchDB3
公证处
Org4
Peer0.Org4
Peer1.Org4
Peer2.Org4
CouchDB0
CouchDB1
CouchDB3
司法鉴定中心
Org5
Peer0.Org5
Peer1.Org5
Peer2.Org5
CouchDB0
CouchDB1
CouchDB3
排序服务
Orderer
Orderer0
Orderer1
Orderer2
Orderer3
Orderer4
Orderer5
Docker/Docker Compose

图2

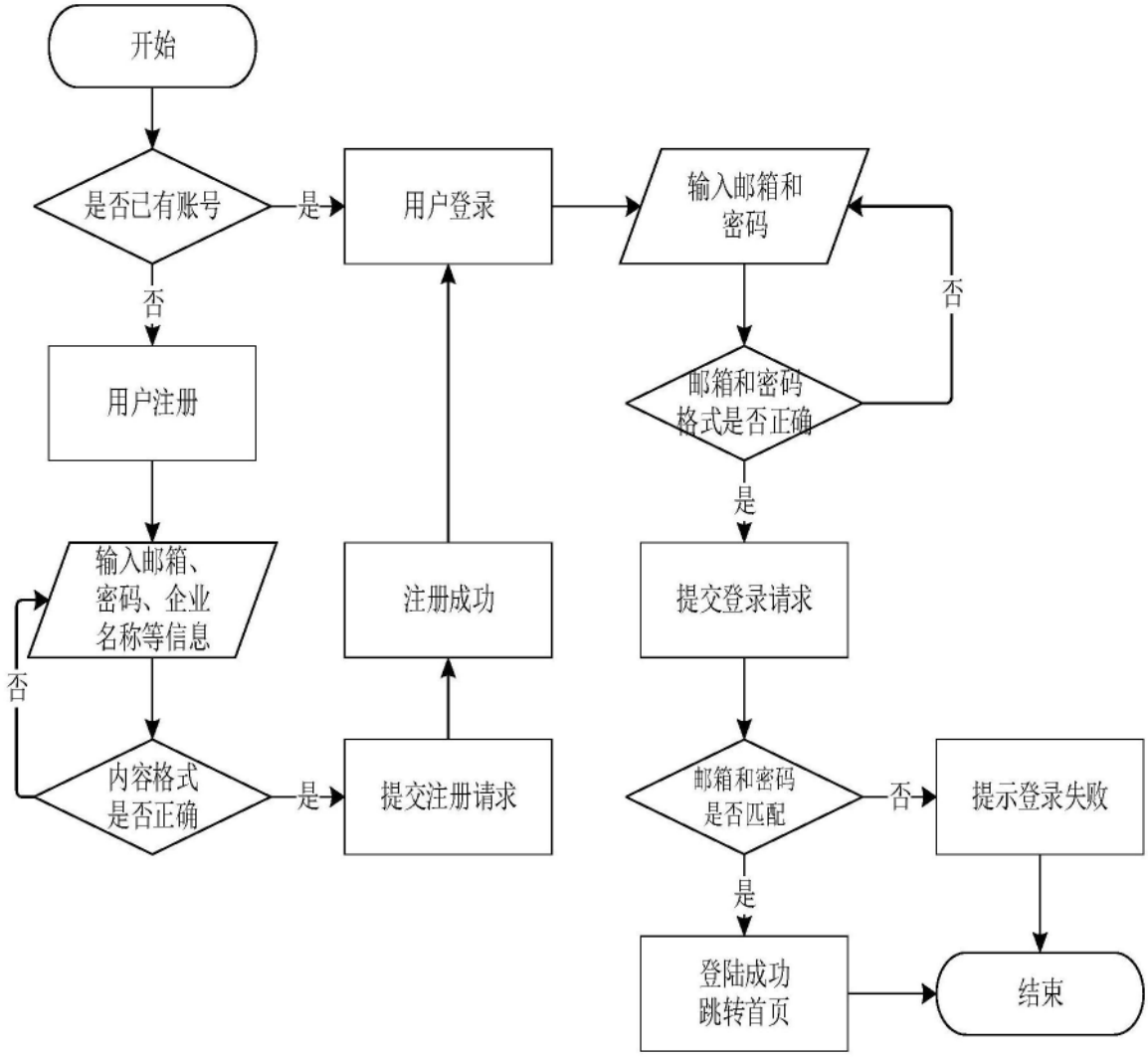

开始
是否已有账号
是
用户登录
输入邮箱和
密码
否
否
用户注册
邮箱和密码
格式是否正确
是
输入邮箱、
密码、企业
名称等信息
注册成功
提交登录请求
否
内容格式
是否正确
是
提交注册请求
邮箱和密码
是否匹配
否
提示登录失败
是
登陆成功
跳转首页
结束

图3

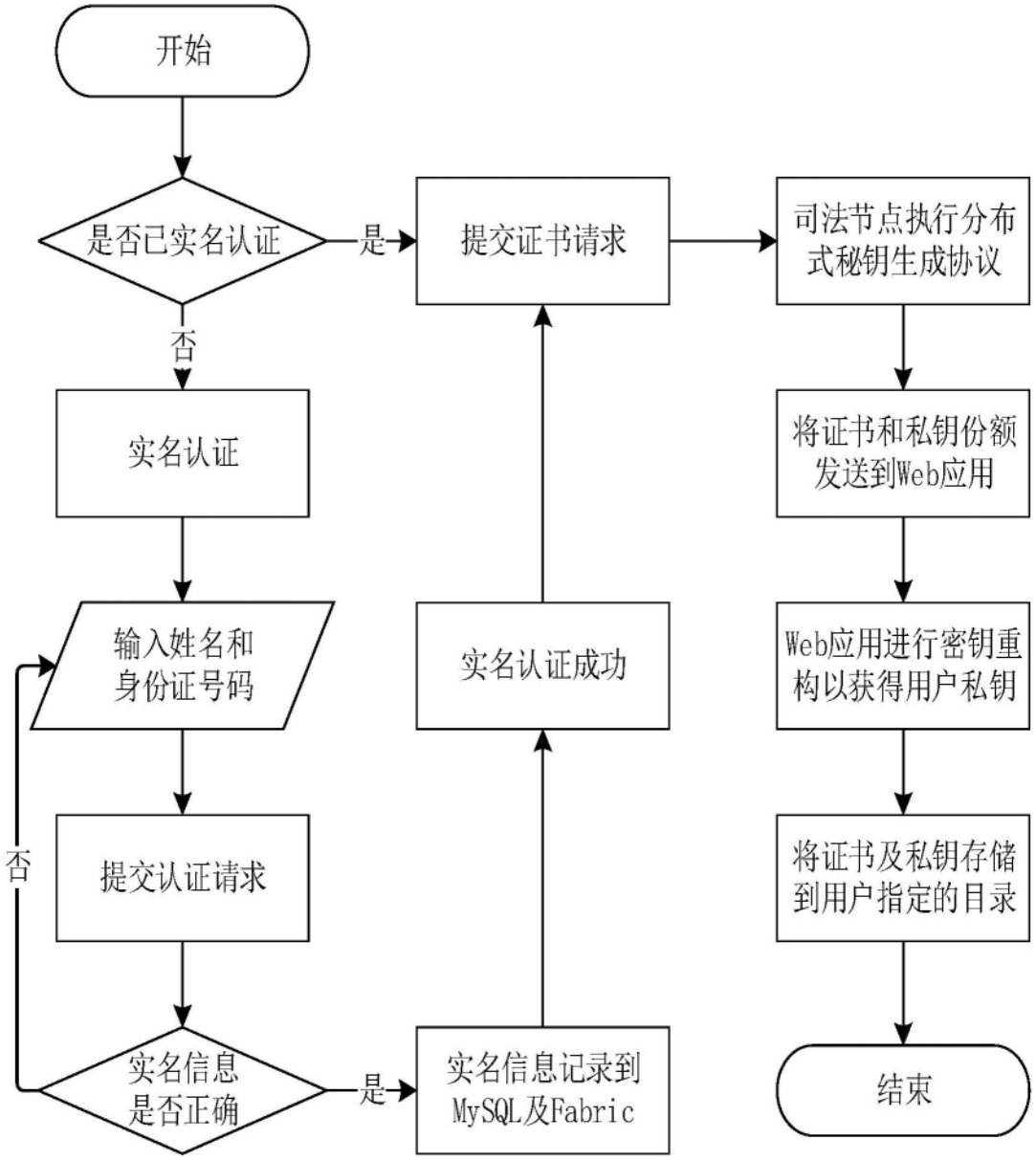

开始
是否已实名认证
是
否
提交证书请求
司法节点执行分布式秘钥生成协议
实名认证
将证书和私钥份额发送到Web应用
输入姓名和身份证号码
实名认证成功
Web应用进行密钥重构以获得用户私钥
提交认证请求
否
将证书及私钥存储到用户指定的目录
实名信息是否正确
是
实名信息记录到MySQL及Fabric
结束

图4

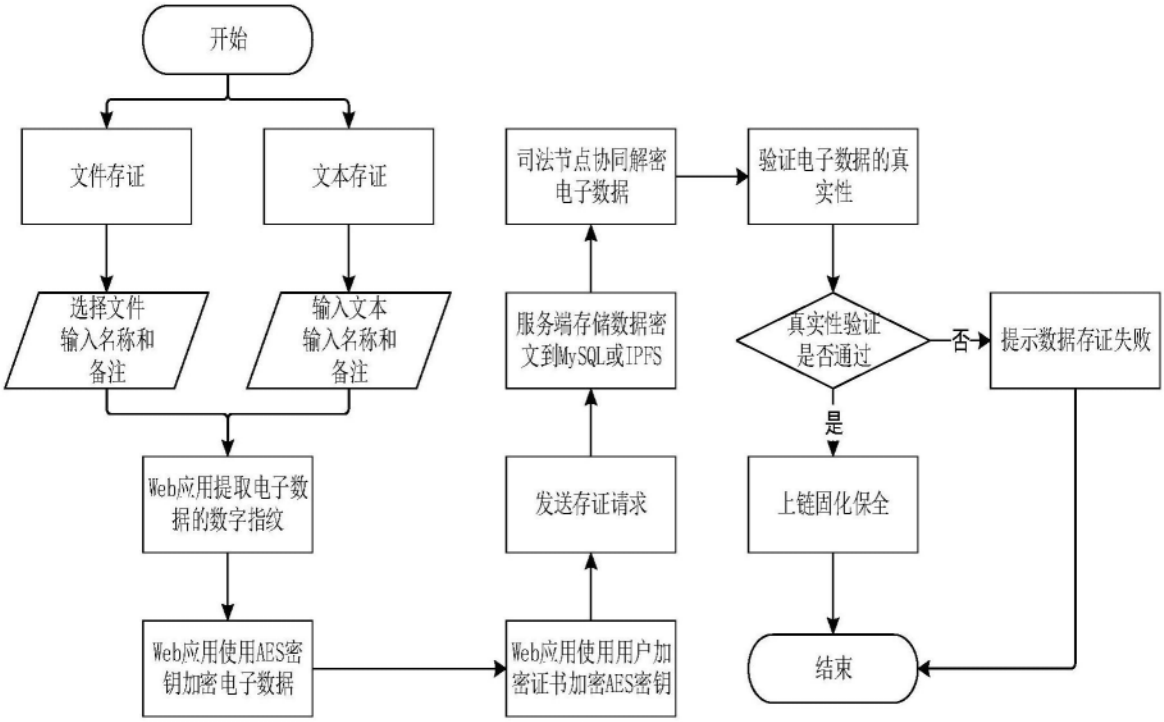

开始
文件存证
文本存证
选择文件
输入名称和
备注
输入文本
输入名称和
备注
Web应用提取电子数
据的数字指纹
Web应用使用AES密
钥加密电子数据
Web应用使用用户加
密证书加密AES密钥
发送存证请求
服务端存储数据密
文到MySQL或IPFS
司法节点协同解密
电子数据
验证电子数据的真
实性
真实性验证
是否通过
否
提示数据存证失败
是
上链固化保全
结束

图5

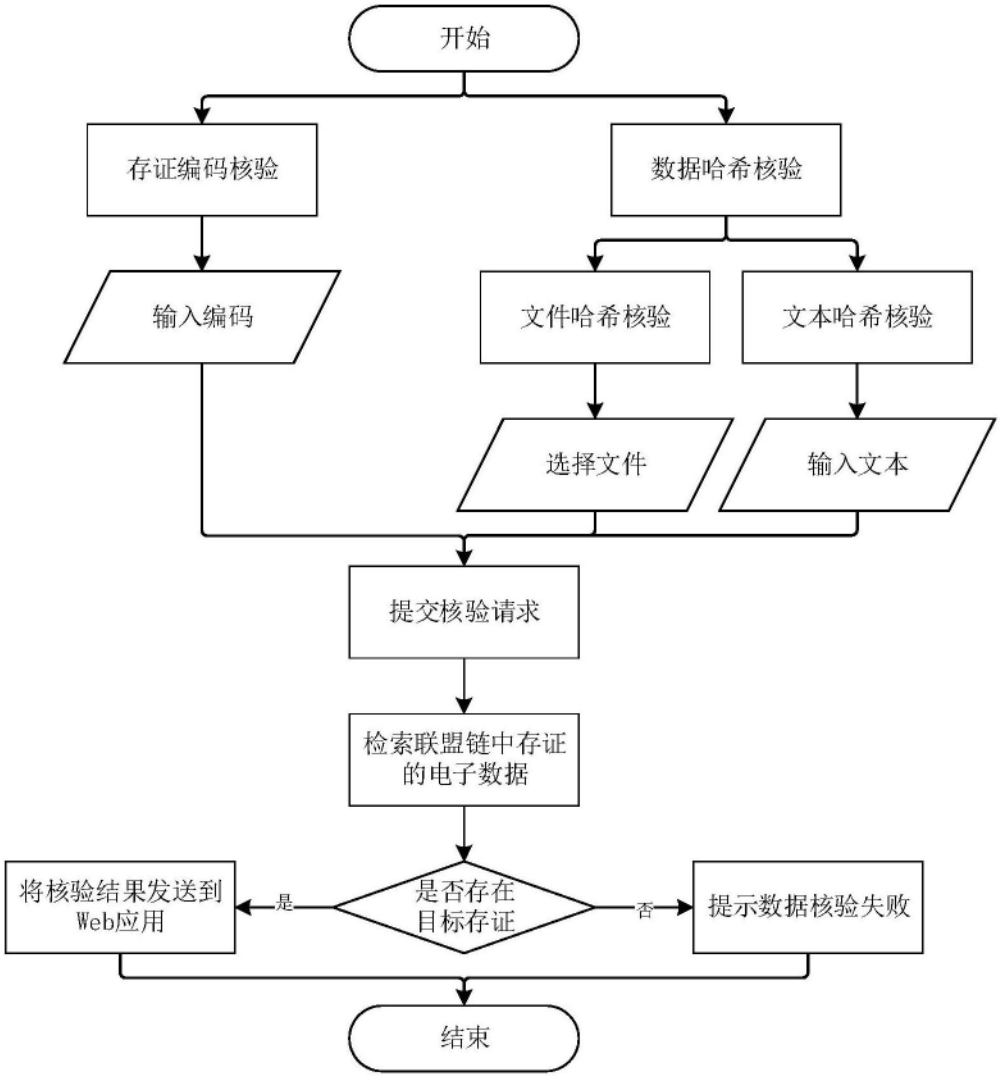

开始
存证编码核验
数据哈希核验
输入编码
文件哈希核验
文本哈希核验
选择文件
输入文本
提交核验请求
检索联盟链中存证的电子数据
将核验结果发送到Web应用
是
是否存在目标存证
否
提示数据核验失败
结束

图6