(19)国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 114710357 A
(43)申请公布日 2022.07.05

(21)申请号 202210378780.8

(22)申请日 2022.04.12

(71)申请人 河北大学
地址 071002 河北省保定市五四东路180号

(72)发明人 杜瑞忠 刘娜 王晶泽

(74)专利代理机构 石家庄国域专利商标事务所有限公司 13112
专利代理师 胡素梅

(51)Int.Cl.
H04L 9/40(2022.01)
H04L 9/32(2006.01)
H04L 67/104(2022.01)

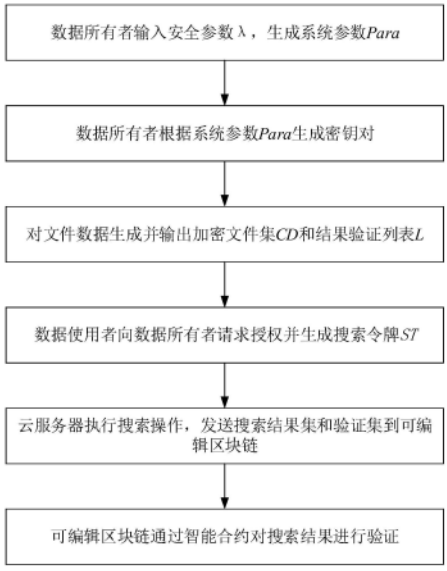
权利要求书2页 说明书9页 附图4页

(54)发明名称

一种可编辑区块链中支持分块验证的动态可搜索加密方法

(57)摘要

本发明提供了一种可编辑区块链中支持分块验证的动态可搜索加密方法。采用端-云与可编辑区块链结合的新方法来替换以前端-云式的数据检索及验证方法。分块索引结构具有很好的检索性能,数据所有者将分块后的验证标签传到可编辑区块链,结果验证功能由可编辑区块链实现。其次,根据分块索引生成的结果验证列表为后续的结果验证减少了计算开销。此外,可编辑区块链技术在保证搜索服务的公平性和安全性的前提下,实现数据的可重写存储,避免区块这一宝贵资源的浪费。本发明可以实现区块链的可编辑性和安全可信性的有机融合。在客户端或者云服务器进行恶意行为时,依然可以确保查询服务的公平性和安全性。



CN 114710357 A

1.一种可编辑区块链中支持分块验证的动态可搜索加密方法,其特征是,包括如下步骤:

A、数据所有者输入安全参数λ,输出系统参数Para;

B、数据所有者根据系统参数Para生成随机数λ_r作为数据更新状态并存储在状态集合Map中,并输出加密所需的密钥对(PK_D,SK_D);

C、对数据所有者的文件进行初始化,根据加密密钥对(PK_D,SK_D),对查询关键字/文件集合进行加密,生成并输出加密索引表$\hat{I}$、加密后的关键字集CW、加密文件集CD到云服务器中,将生成的结果验证列表L存储到可编辑区块链中;

D、当数据使用者发起搜索查询时,将搜索关键字w发送给数据所有者,数据所有者根据搜索关键字w和私钥SK_D为数据使用者发送授权信息;数据使用者根据授权信息生成搜索令牌ST;

E、云服务器接收数据使用者发送的搜索令牌ST执行搜索操作:云服务器首先判断搜索令牌的正确性,若符合条件,则根据加密索引表$\hat{I}$执行搜索操作,并将输出的搜索结果集S_R和验证集P_R发送到可编辑区块链中;

F、可编辑区块链接收到云服务器发送的(S_R,P_R)后,执行验证操作并输出验证结果标识符V_R,通过验证则返回1,可编辑区块链会将搜索结果集发送给数据使用者,并向数据使用者收取费用;否则,返回0,将押金将退还给数据使用者。

2.根据权利要求1所述的可编辑区块链中支持分块验证的动态可搜索加密方法,其特征是,步骤A中,输入安全参数λ,输出双线性对密码参数(G_1,G_2,e,p,g_1);G_1和G_2是两个乘法循环群,p是一个大素数,e为双线性映射$e:G_1\times G_1\rightarrow G_2$,$g_1$是$G_1$的生成数;

定义$H_1:\{0,1\}^*\rightarrow G_1$,$H_2:\{0,1\}^*\rightarrow Z_p$是两个哈希函数,$Z_p$是一个阶为p的有限域,$h_0$和$h_1$均$\in G_1$,得到系统参数Para为$\{G_1,G_2,e,p,g_1,H_1,H_2,h_0,h_1\}$。

3.根据权利要求2所述的可编辑区块链中支持分块验证的动态可搜索加密方法,其特征是,步骤B中,数据所有者从序列$\{1,\cdots,2^{\lambda}\}$中选择随机参数$\lambda_r\in\{1,\cdots,2^{\lambda}\}$作为数据更新状态并记录在状态集合Map中;

数据所有者随机选择一个$x\in Z_p$,并计算非对称随机数密钥对(PK_D,SK_D),其中$PK_D=g_1^x$,$SK_D=x$;

数据所有者存储私钥SK_D,并随机选择参数$\theta\in Z_p$秘密保存;

数据所有者将Map和PK_D均发送给云服务器和可编辑区块链。

4.根据权利要求3所述的可编辑区块链中支持分块验证的动态可搜索加密方法,其特征是,步骤C中,数据所有者首先构建索引结构,所构建的索引结构由若干完美二叉树组成,除最后两棵完美二叉树的高度可能相同外,其他各完美二叉树的高度级联降低;

数据所有者对索引结构按照完美二叉树的个数对其进行分块,分块后计算各块的根结点哈希hr_i以及块索引哈希$h(hr_i)$,并计算σ_i;

$$hr_i=\mathrm{H}(id_1)\oplus\mathrm{H}(id_2)\oplus,\ldots,\oplus\mathrm{H}(id_{ri})$$

$$\sigma_i=\left(h(hr_i)\cdot g_1^{hr_i}\right)^x$$

接着数据所有者根据σ_i计算本地验证标签β_j:

$\beta_j=\prod_{i=1}^{k}\sigma_i^{\lambda_r}$

其中，k为分块后的块数；j＝1,2,……,m,m为关键字个数；

最后生成的结果验证列表为L＝{β_1,β_2,…,β_m}。

5.根据权利要求4所述的可编辑区块链中支持分块验证的动态可搜索加密方法，其特征是，步骤D中，数据使用者将搜索关键字w发送给数据所有者，数据所有者随机选择$\gamma_1\in Z_p$，并计算$d_0=\left(h_0 g_1^{-r_0}\right)^{\frac{1}{x}}\left(h_1^{\bar{w}}\right)^{\gamma_1}$和$d_1=PK_D^{\gamma_1}$；其中，$r_0$＝$H_2$($d_1$)是$Z_p$的一个伪随机数，$\bar{w}=H(w\|\theta)$；$d_0$和$d_1$即为数据所有者向数据使用者所发送的授权信息；数据使用者根据d_0和d_1生成搜索令牌ST＝(d_0,d_1)。

6.根据权利要求5所述的可编辑区块链中支持分块验证的动态可搜索加密方法，其特征是，步骤E中，云服务器判断搜索令牌的正确性具体是：

数据所有者随机的选择x_1,x_2,y∈Z_p，计算$v=e(PK_D,g_1)^{x_1}$和$T=\left(g_1^{y}\right)^{x_1}$，随后，根据v和T计算$\Omega_0=PK_D^{x_2}$，$\Omega_1=ve(g_1,h_0)^{x_2}$，$\Omega_2=e(g_1,g_1)^{x_2}$，并将y、T、$\Omega_0$、$\Omega_1$和$\Omega_2$发送给云服务器；

云服务器接收数据所有者发送的y、T、Ω_0、Ω_1和Ω_2，然后判断搜索令牌ST是否满足$\Omega_1\frac{e\left(d_1,\hat{I}\right)\Omega_2^{-r_0}}{e(\Omega_0,d_0)}==v'$，其中$v'=e(T,PK_D)^{y^{-1}}$；若满足条件，则表示搜索令牌正确。

7.根据权利要求6所述的可编辑区块链中支持分块验证的动态可搜索加密方法，其特征是，步骤E中，当搜索令牌正确时，云服务器根据加密索引表$\hat{I}$执行搜索操作，得到搜索结果集S_R，然后计算验证标签$\mu=\sum_{i=1}^{k}\lambda_r hr_{iCP}$，$hr_{iCP}$为云服务器生成的根结点哈希，同时，云服务器还生成块哈希hr_{1CP},hr_{2CP},…,hr_{kCP}，随后将搜索结果集S_R和验证集P_R＝{h(hr_{1CP}),h(hr_{2CP}),…,h(hr_{kCP}),μ}发送给可编辑区块链。

8.根据权利要求7所述的可编辑区块链中支持分块验证的动态可搜索加密方法，其特征是，步骤F中，可编辑区块链接收数据所有者发送的更新状态λ_r，可编辑区块链收到验证标签P＝(β,μ)以及搜索结果集S_R后，进行结果验证，具体如下：

可编辑区块链根据验证标签，计算V_{D0}＝e(β,g_1)；

并计算$V_{CP}=e\left(\prod_{i=1}^{k}h(hr_{iCP})^{\lambda_r}\cdot g_1^{\mu},PK_D\right)$；

然后可编辑区块链验证V_{CP}＝V_{D0}是否成立；若成立，则将搜索结果集S_R发送给数据使用者；若不成立，则将押金将退还给数据使用者。

9.根据权利要求1-8任一项所述的可编辑区块链中支持分块验证的动态可搜索加密方法，其特征是，该方法还包括步骤G：文件进行更新时，数据所有者生成新的λ_r'记录在Map中，并将更新后的加密索引表$\hat{I}'$、加密关键字集CW′和加密文件集CD′上传到云服务器，更新后的结果验证列表L′使用可编辑技术上传到可编辑区块链。

一种可编辑区块链中支持分块验证的动态可搜索加密方法

技术领域

[0001] 本发明涉及信息安全技术领域,具体地说是一种可编辑区块链中支持分块验证的动态可搜索加密方法。

背景技术

[0002] 可搜索加密(SE,Searchable Encryption)是近年来发展的一种支持用户在密文上进行关键字查找的密码学原语,它能够为用户节省大量的计算和通信开销,并充分利用庞大的计算资源进行密文上的关键字查找。然而在实践中,云服务器和用户并非都是诚实可信的实体。云服务器可能仅返回部分结果以节省计算资源。用户可能为了拒绝支付费用,谎称云服务器的返回结果是错误的。因此存在可靠性问题。

[0003] 为了解决恶意服务器返回给用户错误结果的问题,基于PPTrie树状索引的结果可验证的密文检索方案被提出。随后,将比特币引入多方计算来解决公平问题,方案中的协议可以看作是一个智能合约。为了实现验证的公开化,利用伪随机函数和单向函数来完成。将Merkle Hash Tree与k均值聚类相结合,在提升验证效率的同时也提高了安全性。这些方案假定用户是可信的,会诚实的执行验证过程并发布验证结果。但是有些用户可能谎称结果是错误的,达到拒绝支付服务费的目的。

[0004] 中国专利申请文件(CN113949548A)公开了一种云存储中私钥可验证且多关键词可搜索的属性加密方法,基于属性加密的基础上将可认证外包与关键词搜索加密相结合,有效的减少了本地负荷和计算资源的浪费并实现快速搜索,并且支持多关键词搜索,可以有效地实现快速搜索,解决了现有技术中存在的网络带宽浪费和计算成本较大的问题。

[0005] 中国专利申请文件(CN113282542A)公开了一种具有前向安全的可验证可搜索加密方法,将关键字对应的安全令牌发送给服务器,可防止向服务器暴露文件存储的关键字的相关信息,提高文件存储的安全性,增强对文件注入攻击等不法攻击的抵抗力;确定存储的文件的验证信息,通过验证信息,对服务器返回的搜索到的文件进行完整性校验,能够保证文件存储的完整性,防止服务器对存储的文件的恶意更改;通过生成与验证信息的更新顺序相对应的状态,有利于对验证信息的追溯,便于获得有序的待验证的文件标识符合集,以节省客户端本地对文件标识符的存储操作;通过异或处理的方式,可降低数据处理的复杂度,减少搜索时的通信量,提高搜索效率。

[0006] 目前,区块链技术展示了其解决可靠性问题的潜力。将加密索引和加密数据存储在云服务器,用于实现数据存储和搜索的功能。区块链和智能合约用于验证搜索结果的正确性。由于验证操作都是由网络中的所有结点完成的,因此只要大多数结点都是诚实的,就可以保证结果的正确性。但分布式共享中各个结点之间达成一致的效率很低,智能合约进行复杂计算时产生很大计算开销。区块链的不可更改性导致每次新交易都会产生大量的存储开销,进而影响可搜索加密方案中结果验证的效率、数据更新的性能,降低用户的检索体验。

发明内容

[0007] 本发明的目的就是提供一种可编辑区块链中支持分块验证的动态可搜索加密方法，该方法可在避免区块的存储和计算限制的同时，还能解决由于用户与云服务器不诚实而导致的查询结果可信性的问题。

[0008] 本发明是这样实现的：一种可编辑区块链中支持分块验证的动态可搜索加密方法，包括如下步骤：

[0009] A、数据所有者输入安全参数λ，输出系统参数Para；

[0010] B、数据所有者根据系统参数Para生成随机数λ_r作为数据更新状态并存储在状态集合Map中，并输出加密所需的密钥对(PK_D,SK_D)；

[0011] C、对数据所有者的文件进行初始化，根据加密密钥对(PK_D,SK_D)，对查询关键字/文件集合进行加密，生成并输出加密索引表$\hat{I}$、加密后的关键字集CW、加密文件集CD到云服务器中，将生成的结果验证列表L存储到可编辑区块链中；

[0012] D、当数据使用者发起搜索查询时，将搜索关键字w发送给数据所有者，数据所有者根据搜索关键字w和私钥SK_D为数据使用者发送授权信息；数据使用者根据授权信息生成搜索令牌ST；

[0013] E、云服务器接收数据使用者发送的搜索令牌ST执行搜索操作：云服务器首先判断搜索令牌的正确性，若符合条件，则根据加密索引表$\hat{I}$执行搜索操作，并将输出的搜索结果集S_R和验证集P_R发送到可编辑区块链中；

[0014] F、可编辑区块链接收到云服务器发送的(S_R,P_R)后，执行验证操作并输出验证结果标识符V_R，通过验证则返回1，可编辑区块链会将搜索结果集发送给数据使用者，并向数据使用者收取费用；否则，返回0，将押金将退还给数据使用者。

[0015] 优选的，步骤A中，输入安全参数λ，输出双线性对密码参数(G_1,G_2,e,p,g_1)；G_1和G_2是两个乘法循环群，p是一个大素数，e为双线性映射$e:G_1\times G_1\rightarrow G_2$，$g_1$是$G_1$的生成数；

[0016] 定义$H_1:\{0,1\}^*\rightarrow G_1$，$H_2:\{0,1\}^*\rightarrow Z_p$是两个哈希函数，$Z_p$是一个阶为p的有限域，$h_0$和$h_1$均$\in G_1$，得到系统参数Para为$\{G_1,G_2,e,p,g_1,H_1,H_2,h_0,h_1\}$。

[0017] 优选的，步骤B中，数据所有者从序列$\{1,\cdots,2^{\lambda}\}$中选择随机参数$\lambda_r\in\{1,\cdots,2^{\lambda}\}$作为数据更新状态并记录在状态集合Map中；

[0018] 数据所有者随机选择一个$x\in Z_p$，并计算非对称随机数密钥对(PK_D,SK_D)，其中$PK_D=g_1^x$，$SK_D=x$；

[0019] 数据所有者存储私钥SK_D，并随机选择参数$\theta\in Z_p$秘密保存；

[0020] 数据所有者将Map和PK_D均发送给云服务器和可编辑区块链。

[0021] 优选的，步骤C中，数据所有者首先构建索引结构，所构建的索引结构由若干完美二叉树组成，除最后两棵完美二叉树的高度可能相同外，其他各完美二叉树的高度级联降低；

[0022] 数据所有者对索引结构按照完美二叉树的个数对其进行分块，分块后计算各块的根结点哈希hr_i以及块索引哈希$h(hr_i)$，并计算σ_i；

[0023] $$hr_i=\mathrm{H}(id_1)\oplus\mathrm{H}(id_2)\oplus,\ldots,\oplus\mathrm{H}(id_{ri})$$

[0024] $$\sigma_i=\left(h(hr_i)\cdot g_1^{hr_i}\right)^x$$

[0025] 接着数据所有者根据σ_i计算本地验证标签β_j：

[0026] $\beta_j=\prod_{i=1}^{k}\sigma_i^{\lambda_r}$

[0027] 其中，k为分块后的块数；j＝1,2,……,m,m为关键字个数；

[0028] 最后生成的结果验证列表为L＝{β_1,β_2,…,β_m}。

[0029] 优选的，步骤D中，数据使用者将搜索关键字w发送给数据所有者，数据所有者随机选择$\gamma_1\in Z_p$，并计算$d_0=\left(h_0 g_1^{-r_0}\right)^{\frac{1}{x}}\left(h_1^{\bar{w}}\right)^{\gamma_1}$和$d_1=PK_D{}^{\gamma_1}$；其中，$r_0=H_2(d_1)$是$Z_p$的一个伪随机数，$\bar{w}=H(w\|\theta)$；$d_0$和$d_1$即为数据所有者向数据使用者所发送的授权信息；数据使用者根据d_0和d_1生成搜索令牌ST＝(d_0,d_1)。

[0030] 优选的，步骤E中，云服务器判断搜索令牌的正确性具体是：

[0031] 数据所有者随机的选择x_1,x_2,$y\in Z_p$，计算$v=e(PK_D,g_1)^{x_1}$和$T=\left(g_1^{y}\right)^{x_1}$，随后，根据v和T计算$\Omega_0=PK_D{}^{x_2}$， $\Omega_1=ve(g_1,h_0)^{x_2}$， $\Omega_2=e(g_1,g_1)^{x_2}$，并将y、T、$\Omega_0$、$\Omega_1$和$\Omega_2$发送给云服务器；

[0032] 云服务器接收数据所有者发送的y、T、Ω_0、Ω_1和Ω_2，然后判断搜索令牌ST是否满足$\Omega_1\frac{e(d_1,\hat{I})\Omega_2{}^{-r_0}}{e(\Omega_0,d_0)}==v'$，其中$v'=e(T,PK_D)^{y^{-1}}$；若满足条件，则表示搜索令牌正确。

[0033] 优选的，步骤E中，当搜索令牌正确时，云服务器根据加密索引表$\hat{I}$执行搜索操作，得到搜索结果集S_R，然后计算验证标签$\mu=\sum_{i=1}^{k}\lambda_r hr_{iCP}$，$hr_{iCP}$为云服务器生成的根结点哈希，同时，云服务器还生成块哈希hr_{1CP},hr_{2CP},…,hr_{kCP}，随后将搜索结果集S_R和验证集P_R＝{h(hr_{1CP}),h(hr_{2CP}),…,h(hr_{kCP}),μ}发送给可编辑区块链。

[0034] 优选的，步骤F中，可编辑区块链接收数据所有者发送的更新状态λ_r，可编辑区块链收到验证标签P＝(β,μ)以及搜索结果集S_R后，进行结果验证，具体如下：

[0035] 可编辑区块链根据验证标签，计算V_{D0}＝e(β,g_1)；

[0036] 并计算$V_{CP}=e\left(\prod_{i=1}^{k}h(hr_{iCP})^{\lambda_r}\cdot g_1{}^{\mu},PK_D\right)$；

[0037] 然后可编辑区块链验证V_{CP}＝V_{D0}是否成立；若成立，则将搜索结果集S_R发送给数据使用者；若不成立，则将押金将退还给数据使用者。

[0038] 优选的，本发明所提供的可编辑区块链中支持分块验证的动态可搜索加密方法还包括步骤G：文件进行更新时，数据所有者生成新的λ_r'记录在Map中，并将更新后的加密索引表$\hat{I}'$、加密关键字集CW′和加密文件集CD′上传到云服务器，更新后的结果验证列表L′使用可编辑技术上传到可编辑区块链。

[0039] 本发明将加密的数据和索引存储在云服务器，结果验证列表存储在可编辑区块链，避免区块的存储和计算限制的同时，解决了由于用户与云服务器不诚实而导致的查询结果可信性的问题。本发明的主要贡献如下：

[0040] 1)为了保证高效的查询和验证，对索引进行动态划分，利用分块索引实现并行搜索以及更新数据仅影响恒定数量数据。此外，利用分块索引生成的验证标签对查询结果进行分块验证。

[0041] 2)引入可编辑区块链技术，使拥有修改权限的实体(本发明指数据所有者)可更改

区块数据,便于维护验证标签的上传和更新,提高结果验证效率的同时减少验证标签的存储开销。

[0042] 3)本发明能够阻止云服务器通过搜索陷门来猜测关键字的具体信息,实现搜索模式隐私保护。

[0043] 4)通过部署到本地私有测试网络(Ganache-cli)中,并且对数据进行分梯度实验。实验结果分析表明,本发明在保证区块数量低速率增长前提下,数据查询和验证性能较其他结果验证方案优势显著。

[0044] 本发明基于可编辑区块链构建了支持分块验证的动态可搜索加密方法。该方法具有如下优势:首先,分块索引结构具有很好的检索性能;其次,根据分块索引生成的结果验证列表为后续的结果验证减少了计算开销;第三,可编辑区块链技术在保证搜索服务的公平性和安全性的前提下,实现数据的可重写存储,避免区块这一宝贵资源的浪费。

附图说明

[0045] 图1是本发明的系统模型图。

[0046] 图2是本发明方法的简约流程图。

[0047] 图3是本发明方法细化后的流程图。

[0048] 图4是本发明各实体间数据传输的示意图。

[0049] 图5是本发明索引结构中添加以及删除结点的示意图。

[0050] 图6是本发明对索引结构进行分块的示意图。

具体实施方式

[0051] 为了使本发明的目的、技术方案及优点更加清楚,以下结合附图及实施例,对本发明进行进一步详细说明。

[0052] 为了保证搜索结果的正确性和完整性,本发明引入可编辑区块链作为第三方可信实体。同时,为了不削弱云存储的优势,应使结果验证的开销尽可能小。为了实现以上功能,本发明动态划分索引结构,块索引间并行计算生成验证标签。将验证标签组成的结果验证列表L上传到可编辑区块链中,对云服务器检索的结果进行验证。该验证方式不仅能提高验证标签生成效率、减小列表L的大小,还能降低可编辑区块链验证过程中的计算开销;此外,使用可编辑技术维护L的更新,还能最小化区可编辑块链存储开销。

[0053] 如图1所示,本发明系统模型包含数据所有者(DO,Data Owner)、数据使用者(DU,Data User)、云服务器(CSP,Cloud Server Platform)以及可编辑区块链(Redactable Blockchain)四个实体。可编辑区块链简称区块链,数据使用者即数据用户(简称用户),云服务器也即云平台(CP,Cloud Platform)。数据所有者可以构建安全的索引和密文文件,并上传到云服务器。同时,数据所有者还可以将生成的结果验证列表L上传到可编辑区块链。在数据使用者提出搜索请求后,数据所有者为合法用户授权。具有搜索权限的数据使用者可以生成令牌并向云服务器提交搜索查询,并可接收区块链发送来的通过验证的搜索结果集,在本地进行解密。云服务器用来存储安全索引和密文文件,同时可以为数据使用者提供搜索服务。执行搜索算法得到搜索结果发送给区块链,供其验证结果正确性。用户对数据的操作都被视为交易过程,该过程通过智能合约(SC,Smart Contract)打包到可编辑区块链

中。智能合约属于可编辑区块链，可编辑区块链中的很多操作都是依据智能合约来完成的。智能合约通过结果验证列表L对云服务器得到的搜索结果进行验证，然后将验证通过的搜索结果发送给数据使用者。使用可编辑技术完成对结果验证列表L的更新操作，实现区块链数据在交易级别上的细粒度修改，保证区块数量低速率增长。

[0054] 可编辑区块链是区块链领域新兴的热点，旨在保障区块链安全可信等良好性质的前提下实现链上数据的可控编辑操作。本发明将区块链的内哈希函数替换为变色龙哈希函数，利用变色龙哈希的碰撞性实现区块的可编辑。

[0055] 变色龙哈希函数是一种带陷门的单向哈希函数。如果掌握陷门信息，则可以轻易地计算任意输入数据的哈希碰撞，从而可以在不改变哈希函数输出的情况下，任意地改变哈希函数的输入。

[0056] 变色龙哈希函数通常有如下四个算法，即密钥生成算法HG、哈希生成算法CH、哈希验证算法HV以及哈希碰撞算法HC。四个算法分别如下：

[0057] 1)$HG(1^n)=(hk,tk)$：生成变色龙哈希的公钥hk和私钥(陷门)tk，n为安全性参数。

[0058] 2)$CH(hk,x,r)=(h,\xi)$：给定公钥hk、任意数据x和随机数r，生成哈希值h和随机数ξ。

[0059] 3)$HV(hk,x,(h,\xi))$：给定公钥hk、任意数据x、哈希值h和随机数ξ，如果(h,ξ)是正确的哈希值，则输出1，否则输出0。

[0060] 4)$HC(tk,(h,x,\xi),x')$：给定陷门tk、三元组(h,x,ξ)和数据x′，输出新随机数ξ′，使得$HV(hk,x,(h,\xi))=HV(hk,x',(h,\xi'))=1$。

[0061] 显然，掌握陷门密钥就意味着拥有区块链的修改权，因此陷门密钥的管理对于变色龙哈希函数来说至关重要。

[0062] 如图2所示，本发明的可编辑区块链中支持分块验证的动态可搜索加密方法包括以下步骤：

[0063] A、数据所有者输入安全参数λ，输出公共系统参数Para，该公共系统参数Para可被各实体获知。

[0064] B、数据所有者根据公共系统参数Para生成随机数λ_r作为数据更新状态标识符并存储在状态集合Map中，并输出加密所需的密钥对(PK_D,SK_D)。

[0065] C、对数据所有者的文件进行初始化，根据加密密钥对(PK_D,SK_D)，对查询关键字/文件集合(W/F)进行加密，生成并输出加密索引表$\hat{I}$、加密后的关键字集CW、加密文件集CD到云服务器中，将生成的结果验证列表L存储到可编辑区块链中。

[0066] D、当数据使用者发起搜索查询时，将搜索关键字w发送给数据所有者，数据所有者根据搜索关键字w和私钥SK_D为数据使用者发送授权信息；数据使用者根据授权信息生成搜索令牌ST。

[0067] E、云服务器执行搜索操作，云服务器接收数据使用者发送的搜索令牌ST。首先判断令牌的正确性，若符合条件，则根据加密索引表$\hat{I}$执行搜索操作，并将输出的搜索结果集S_R和验证集P_R发送到可编辑区块链中。

[0068] F、可编辑区块链接收到云服务器发送的(S_R,P_R)后，执行验证操作并输出验证结果标识符V_R，通过验证则返回1，可编辑区块链会将搜索结果发送给数据使用者，并向数据使用者收取费用；否则，返回0，将押金将退还给数据使用者。

[0069] 本发明所提供的动态可搜索加密方法还包括更新步骤，如下：

[0070] G、文件进行更新时，数据所有者生成新的λ_r'记录在Map中，并将更新后的加密索引表$\hat{I}'$、加密关键字集CW′和加密文件集CD′上传到云服务器，更新后的结果验证列表L′使用可编辑技术上传到可编辑区块链。

[0071] 下面结合附图对各个步骤进行详细描述。

[0072] 结合图2、图3和图4，在步骤A中，输入安全参数λ，设G_1和G_2是两个乘法循环群，p是一个大素数，e为双线性映射$e:G_1\times G_1\rightarrow G_2$，$g_1$是$G_1$的生成数。输出双线性对密码参数$(G_1,G_2,e,p,g_1)$。

[0073] 定义$H_1:\{0,1\}^*\rightarrow G_1$，$H_2:\{0,1\}^*\rightarrow Z_p$是两个哈希函数，$Z_p$是一个阶为p的有限域，$h_0$和$h_1$均$\in G_1$，得到公共系统参数为$Para=\{G_1,G_2,e,p,g_1,H_1,H_2,h_0,h_1\}$。

[0074] 在步骤B中，数据所有者在本地初始化系统，数据所有者根据公共系统参数Para，从序列$\{1,\cdots,2^{\lambda}\}$中选择随机参数$\lambda_r\in\{1,\cdots,2^{\lambda}\}$作为数据更新状态记录在状态集合Map中。$\lambda_r$作为数据更新状态标识符，用来表示数据是否实现更新。

[0075] 随机选择一个$x\in Z_p$，并计算数据所有者的非对称随机数密钥对(PK_D,SK_D)，其中$PK_D=g^x$，$SK_D=x$。数据所有者存储私钥SK_D，并随机选择参数$\theta\in Z_p$秘密保存。此外，数据所有者将Map和PK_D均发送给云服务器和可编辑区块链。

[0076] 在步骤C中，数据所有者不仅需要对关键字/文件集合(W/F)加密来建立索引，还需要利用分块索引产生用于结果验证的列表L。

[0077] 数据所有者将文件关键字集$W=\{w_1,w_2,\cdots,w_m\}$和文件集$F=\{f_1,f_2,\cdots,f_n\}$作为输入，选择一个安全的对称加密算法$Enc=(E_k,D_k)$对文件进行加密，加密后的文件为$C_j=E_k(f_j)$，$j=1,2,\cdots,n$。其中，m为关键字数量；n为文件数。对关键字w加密具体是执行如下操作：$\bar{w}=H(w\|\theta)$，“||”表示“或”，关键字w和θ取或，再计算哈希，得到加密后的关键字$\bar{w}$。

[0078] 本发明采用索引分块实现并行操作，在执行过程中通过并行遍历加快检索速率、方便检查结果验证列表L的生成以及后续的验证操作，使得在查询和验证性能上优势显著。通过分块索引结构对可搜索加密的结果进行分块验证，有效减少客户端的计算开销、存储开销以及通信开销。

[0079] 本发明中索引结构由多个完美二叉树(除叶子结点之外的每一个结点都有两个孩子，每一层都被完全填充)组成。在构建索引过程中，关键字/文档标识符对(w,id)依序添加，故树形成过程中有先后顺序。除了最后两棵树的高度可能相等外，其他所有的二叉树高度严格降低(级联)，此特性将在后续的更新中得到维护。对于任何关键字w，将包含w的文件标识符集打包为多个完美二叉树(三角形)，则最大完美二叉树形成，已经形成二叉树的文件标识符被减去以继续形成下一个最大的完美二叉树。因此，除了最后两棵完美二叉树的高度可能相同，其余二叉树的高度依次减少。如图5所示，如果要添加关键字/文档标识符对(w,id)，则新添加的结点将作为两个相同高度的完美二叉树的父结点。否则，新结点是高度为1的完美二叉树。要删除(w,id)，则是将其替换为最后一个完美二叉树的根结点，并将最小的完美二叉树分成两个较小的二叉树。可以看到，添加和删除后的级联特性没有改变。最后，任何(并行)树遍历算法都可以遍历该数据结构，因此这种结构可以实现并行查询和数据更新，并且具有更新数据仅影响恒定数量数据的特性。

[0080] 对每一个关键字均执行上述索引结构的建立过程。之后对于关键字集合W中的每

个元素w_j(1≤j≤m)生成的倒排索引进行索引分块,1≤i≤k(k是索引分块块数)。如图6所示,将索引结构中的每个完美二叉树划分成一个块,因此k即为完美二叉树的个数。图6中k=3,索引结构中结点数为11;分块后的索引结构为I={I_1,I_2,I_3}。如果根据划分后的块生成的结果验证列表进行结果验证时仍旧超过以太坊的Gas限值,则在此块的基础上,将其分为三个子树(块)。如图6中的块索引I_1,再次划分的子树分别是根结点($Root_0$)和除去根结点以外,其左右子结点(左子结点Chd_{00}和右子结点Chd_{01})重新生成的索引结构。二次划分方式在块内部自行划分,从外部看仍然为整体块结构。如图6中,对I_1进行二次分块后有I_1={$Root_0$,Chd_{00},Chd_{01}}。这种分块方式可以实现动态划分,并且有效避免存储浪费。然后根据分块后的结果来计算加密后的根结点哈希$hr_i = \mathrm{H}(id_1)\oplus\mathrm{H}(id_2)\oplus,\ldots,\oplus\mathrm{H}(id_{ri})$,然后数据所有者针对根结点哈希,计算块索引哈希h(hr_i)以及σ_i。其中,$\sigma_i=\left(h(hr_i)\cdot g_1^{hr_i}\right)^x$。上面公式中,“⊕”表示异或,H($id_{ri}$)表示第$r_i$个文档标识符的哈希值,$hr_i$表示第i个块的根结点哈希,h($hr_i$)表示块索引哈希。对于某一个确定的块i,其上拥有$r_i$个结点,计算$hr_i$即计算该块上所有结点中文档标识符的哈希值,再进行异或。最后,数据所有者将密文以及加密索引$\hat{I}$上传至云服务器。

[0081] 接着,数据所有者根据σ_i在本地计算验证标签β_j,具体为$\beta_j=\prod_{i=1}^{k}\sigma_i^{\lambda_r}$。最终得到与所有关键字相对应的结果验证列表L={$\beta_1$,$\beta_2$,…,$\beta_m$}。数据所有者将结果验证列表L发送到可编辑区块链。可编辑区块链接收到数据所有者发送的结果验证列表L后,根据公钥hk、验证标签β_j和随机数r,计算CH(hk,β_j,r)=(h,ξ),并存储生成的哈希值h和随机数ξ。

[0082] 步骤D中,当数据使用者发起搜索查询时,首先需要向数据所有者请求搜索权限,即:数据使用者将搜索关键字w发送给数据所有者。数据所有者随机选择$\gamma_1\in Z_p$,并计算$d_0=\left(h_0 g_1^{-r_0}\right)^{\frac{1}{x}}\left(h_1^{\bar{w}}\right)^{\gamma_1}$和$d_1=PK_D^{\gamma_1}$;其中,$r_0$=$H_2$($d_1$)是$Z_p$的一个伪随机数,$\bar{w}=H(w\|\theta)$。数据所有者将授权信息$d_0$和$d_1$发送给数据使用者,由数据使用者生成搜索令牌ST=(d_0,d_1)。数据使用者将搜索令牌ST发送给云服务器。

[0083] 数据所有者随机的选择x_1,x_2,y∈Z_p,计算$v=e(PK_D,g_1)^{x_1}$和$T=\left(g_1^{y}\right)^{x_1}$,随后,根据v和T计算$\Omega_0=PK_D^{x_2}$, $\Omega_1=ve(g_1,h_0)^{x_2}$, $\Omega_2=e(g_1,g_1)^{x_2}$,并将y、T、$\Omega_0$、$\Omega_1$和$\Omega_2$发送给云服务器,以便云服务器对数据使用者发送的搜索令牌的有效性进行校验。

[0084] 步骤E中,云服务器获取加密索引$\hat{I}$和加密关键字集CW后进行如下计算,在搜索关键字之前,首先判断数据使用者发送的搜索令牌ST是否满足$\Omega_1\frac{e(d_1,\hat{I})\Omega_2^{-r_0}}{e(\Omega_0,d_0)}==v'$,其中$v'=e(T,PK_D)^{y^{-1}}$。若满足条件,则表示搜索令牌正确。若搜索令牌不正确,则云服务器反馈给数据使用者。

[0085] 若搜索令牌正确,则云服务器接下来判断$\lambda_r=\lambda_{rCP}$是否成立,λ_r表示数据所有者生成的最新的更新标识符,λ_{rCP}表示本次查询前的上一次查询时的更新标识符,两者相等,则表示两次查询之间没有发生过更新。因此,若$\lambda_r=\lambda_{rCP}$成立,则表示未发生更新,此时由云服务器根据未更新的加密索引$\hat{I}$执行搜索。若$\lambda_r=\lambda_{rCP}$不成立,则表示关键字由更新后的新索

引生成，此时需由云服务器根据更新后的加密索引$\hat{I}'$执行并行搜索算法。

[0086] 云服务器根据加密索引(未更新的或更新后的加密索引)执行搜索算法，具体是：当索引块数k≥1时，初始化$\overline{CD}=\perp$，$\overline{FID}=\perp$，⊥代表空集，对于j＝1,2,…,k，若左右子树均不为空$chd_{00}\neq\perp$($\vee chd_{01}\neq\perp$)(“∨”为析取符号，表示“或”，chd_{00}表示左子树，chd_{01}表示右子树)，则对每棵完美二叉树执行中序遍历算法，计算$\overline{CD}=\overline{CD}\cup\overline{CD}'$，$\overline{FID}=\overline{FID}\cup\overline{FID}'$。$\overline{CD}'$和$\overline{FID}'$是满足搜索令牌的文件和文件标识符，$\overline{CD}$和$\overline{FID}$是满足搜索令牌的文件集和文件标识符集，$S_R=(\overline{CD},\overline{FID})$是搜索结果集。

[0087] 云服务器根据S_R，索引$I=\{I_1,I_2,\cdots I_k\}$，计算验证标签$\mu=\sum_{i=1}^{k}\lambda_r hr_{iCP}$，$hr_{iCP}$为云服务器生成的根结点哈希，同时，云服务器还生成块哈希$hr_{1CP},hr_{2CP},\cdots,hr_{kCP}$。随后将搜索结果集$S_R$和验证集$P_R=\{h(hr_{1CP}),h(hr_{2CP}),\cdots,h(hr_{kCP}),\mu\}$发送给可编辑区块链。

[0088] 步骤F中：可编辑区块链接收数据所有者发送的更新状态λ_r，可编辑区块链收到验证标签$P=(\beta,\mu)$以及搜索结果集S_R后，进行结果验证，具体如下：

[0089] 可编辑区块链根据本地验证标签β，计算$V_{DO}=e(\beta,g_1)$；

[0090] 并根据云服务器生成的验证标签μ计算$V_{CP}=e\left(\prod_{i=1}^{k}h(hr_{iCP})^{\lambda_r}\cdot g_1^{\mu},PK_D\right)$。

[0091] 然后验证$V_{CP}=V_{DO}$是否成立。

[0092] 如果$V_{CP}=V_{DO}$，即

[0093]
$$V_{DO}=e(\beta,g_1)=e\left(\prod_{i=1}^{k}\sigma_i^{\lambda_r},g_1\right)=e\left(\prod_{i=1}^{k}\left(h(hr_i)\cdot g_1^{hr_i}\right)^{x\lambda_r},g_1\right)$$

$$=e\left(\prod_{i=1}^{k}h(hr_i)^{\lambda_r}\cdot\prod_{i=1}^{k}g_1^{hr_i\lambda_r},g_1^{x}\right)=e\left(\prod_{i=1}^{k}h(hr_{iCP})^{\lambda_r}\cdot g_1^{\mu},PK_D\right)=V_{CP}$$

[0094] 则表示搜索结果正确，验证结果输出$V_R=1$，可编辑区块链将搜索结果以及λ_r记录下来，并将搜索结果发送给数据使用者，并向数据使用者收取费用，数据使用者根据搜索结果在本地解密(数据所有者需将对称加密密钥发送给数据使用者)。如果证$V_{CP}=V_{DO}$不成立，则输出$V_R=0$，可编辑区块链将押金退还给数据使用者(数据使用者在获得授权信息后支付押金)。

[0095] 步骤G中，数据所有者获取关键字w对应的更新状态，若$\lambda_r'\neq\lambda_r$(λ_r'代表新的更新后的状态)，则执行下面的更新操作。

[0096] 令W′，F′表示更新后的关键字集和文档集，选择一个安全的对称加密算法$Enc=(E_k,D_k)$，计算加密后的文件$CD'=E_k(F')$。

[0097] 对于集合W′中的每个元素w_j'($1\leq j\leq m$)，执行加密算法得到加密索引$\hat{I}'$。根据更新后的索引，并行执行相应计算过程，生成新的本地验证标签β_i'以及结果验证列表L′。

[0098] 将更新后的λ_r'和L′上传到可编辑区块链。首先，给定安全参数λ，计算

[0099] $(hk,tk)=HG(1^{\lambda})$

[0100] 生成变色龙哈希的公钥hk和私钥(陷门)tk。

[0101] 接着，计算新的随机数

[0102] $\xi'=HC(tk,(h,\beta_i,\xi),\beta_i')$

[0103] 然后，验证$HV(hk,\beta_i,(h,\xi))=HV(hk,\beta_i',(h,\xi'))=1$是否成立。

[0104] 如果成立，那么，使用可编辑技术更新本地验证标签成功。

[0105] 本发明中，属于可编辑区块链的智能合约是“执行合约条款的计算机交易协议”。具体来说，智能合约系统的每个参与者都运行一个基于交易的状态机，从一个创世状态开始，在区块链上执行交易以将其转变为某个最终状态。由于区块链上只包含有效交易，因此最终状态可以在所有参与者之间自动达成共识。本发明用于根据分块索引生成的检查列表(即结果验证列表)的上传及后续更新，以及用于实现数据的可重写存储而采用的可编辑技术，都是在智能合约中实现的。主要的智能合约有四个，分别为：可编辑区块链合约、检查列表更新合约、公平交易合约和结果验证合约。其中，可编辑区块链合约和检查列表更新合约用于实现检查列表的上传与更新，公平交易合约与结果验证合约确保公平性和结果可验证性。

[0106] 本发明可达到保护用户隐私以及数据安全的目的。本发明的安全目标是强制执行以下约束条件而得到的：

[0107] 1)隐私性。在整个搜索过程中，文件和查询关键字保密。云服务器和可编辑区块链都不能够推断出客户端的私有文件和发布的搜索关键字。

[0108] 2)安全性。在程序执行期间，确保除了一系列搜索请求、更新请求和访问模式的结果之外，没有其他信息被披露。本发明将更新操作的结果也视为搜索模式的一部分。

[0109] 3)验证性。需要对恶意用户以及恶意云服务器进行双向验证，将验证过程交由可编辑区块链去执行，保证各个实体的诚实操作。

[0110] 4)公平性。如果用户和云服务器发生纠纷，可以公平地检测出确切的错误行为者，并强制执行公平交易。也就是说，如果确认云服务器错误地执行了所请求的搜索查询，则应拒绝支付该查询的服务费。反之，如果确认用户伪造了验证结果，则应强制执行本次查询的服务费。

[0111] 本发明提出的可编辑区块链架构平台、操作功能和公平支付机制是使用Python和以太坊智能合约实现的。本发明在用户和服务器进行恶意行为时，依然可以确保查询服务的公平性和安全性。实验结果表明本发明具有良好的查询性能、验证性能和存储性能。

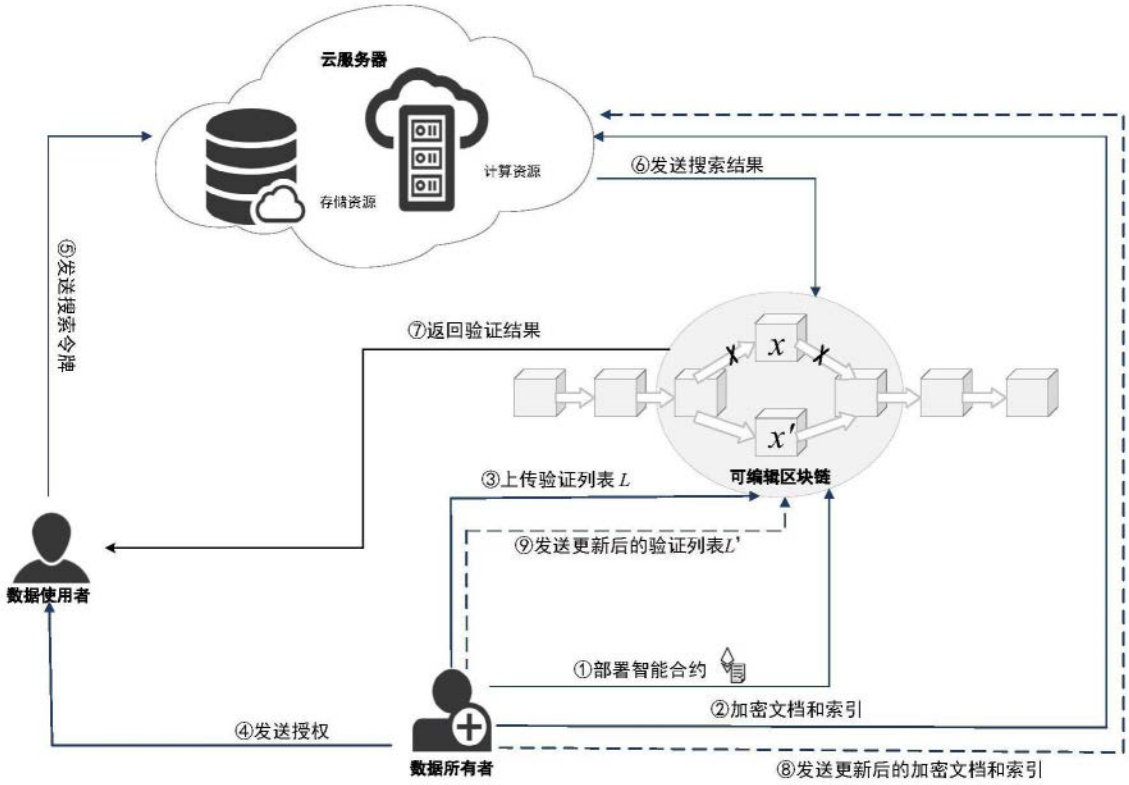

云服务器
存储资源
计算资源
⑥发送搜索结果
⑤发送搜索令牌
⑦返回验证结果
x
x'
可编辑区块链
③上传验证列表 L
⑨发送更新后的验证列表L'
数据使用者
①部署智能合约
②加密文档和索引
④发送授权
数据所有者
⑧发送更新后的加密文档和索引

图1

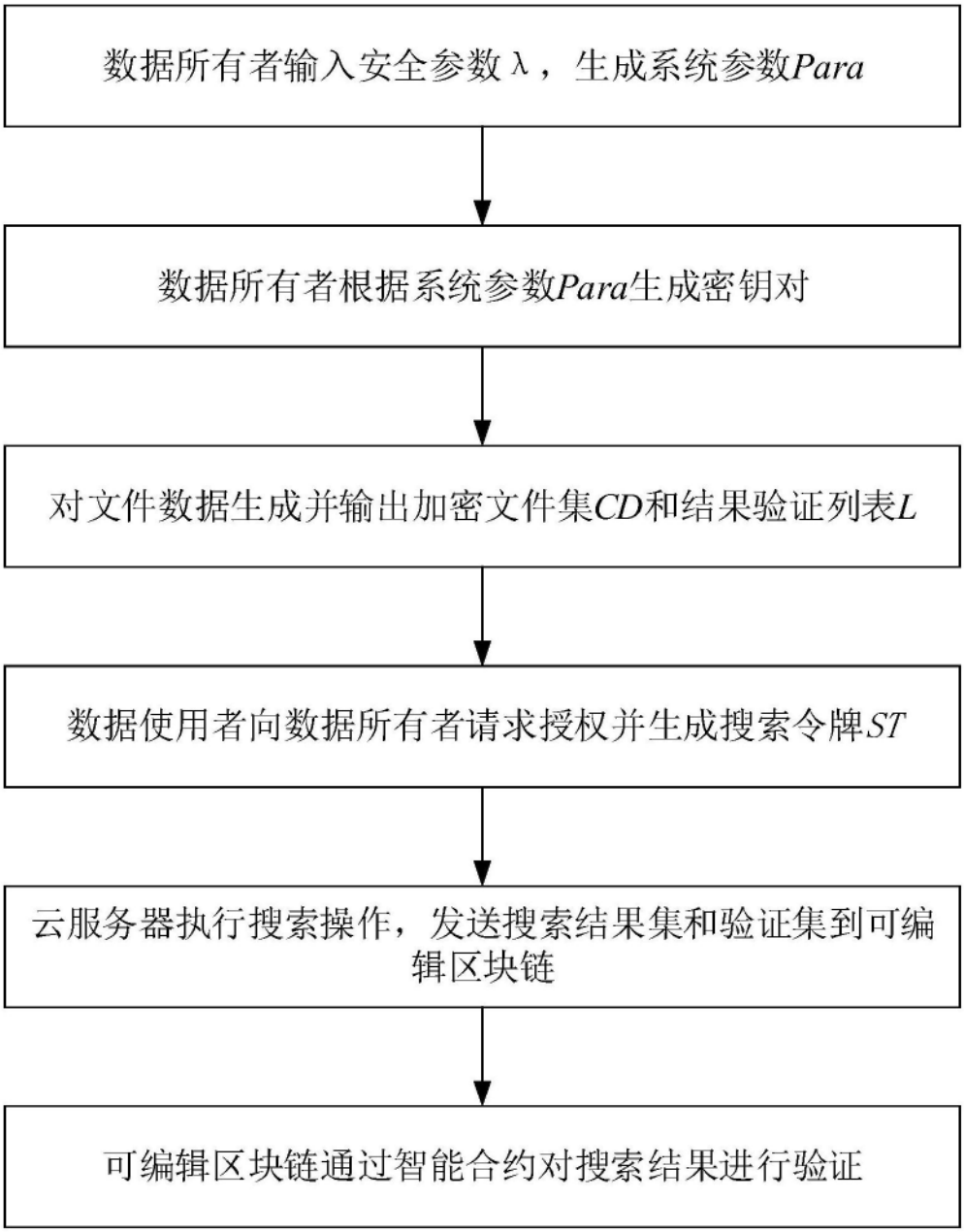

数据所有者输入安全参数λ，生成系统参数*Para*
数据所有者根据系统参数*Para*生成密钥对
对文件数据生成并输出加密文件集*CD*和结果验证列表*L*
数据使用者向数据所有者请求授权并生成搜索令牌*ST*
云服务器执行搜索操作，发送搜索结果集和验证集到可编辑区块链
可编辑区块链通过智能合约对搜索结果进行验证

图2

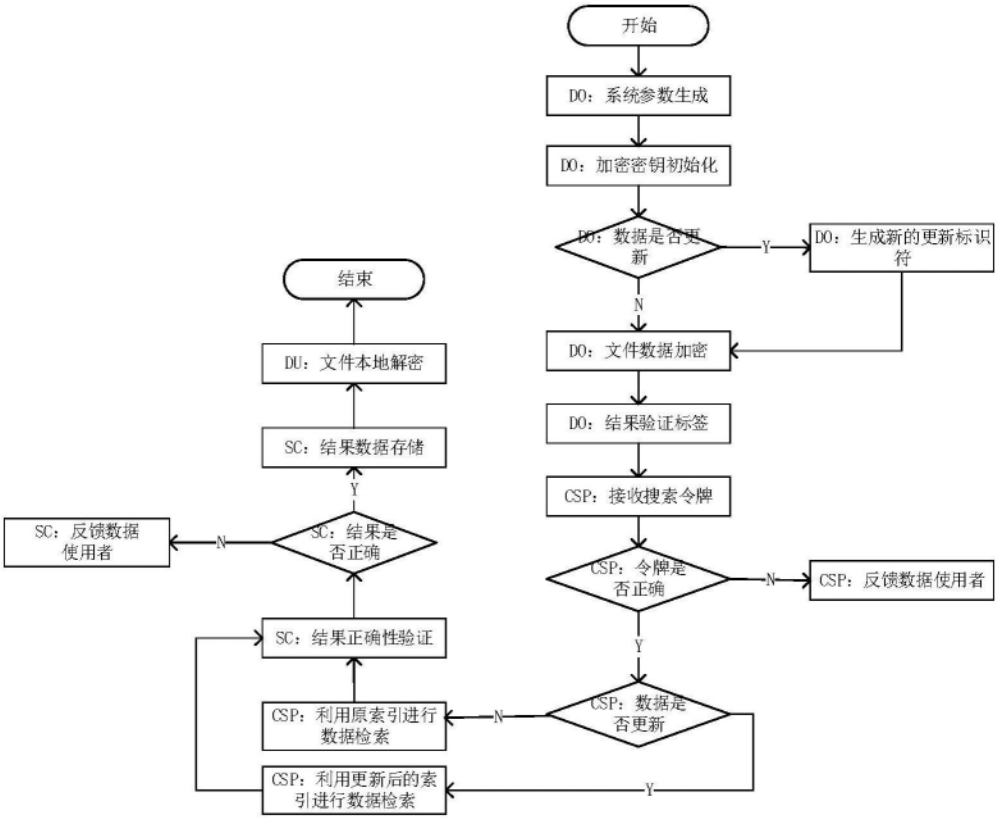

开始
DO：系统参数生成
DO：加密密钥初始化
DO：数据是否更新
Y
DO：生成新的更新标识符
N
DO：文件数据加密
DO：结果验证标签
CSP：接收搜索令牌
CSP：令牌是否正确
N
CSP：反馈数据使用者
Y
CSP：数据是否更新
N
CSP：利用原索引进行数据检索
Y
CSP：利用更新后的索引进行数据检索
SC：结果正确性验证
SC：结果是否正确
N
SC：反馈数据使用者
Y
SC：结果数据存储
DU：文件本地解密
结束

图3

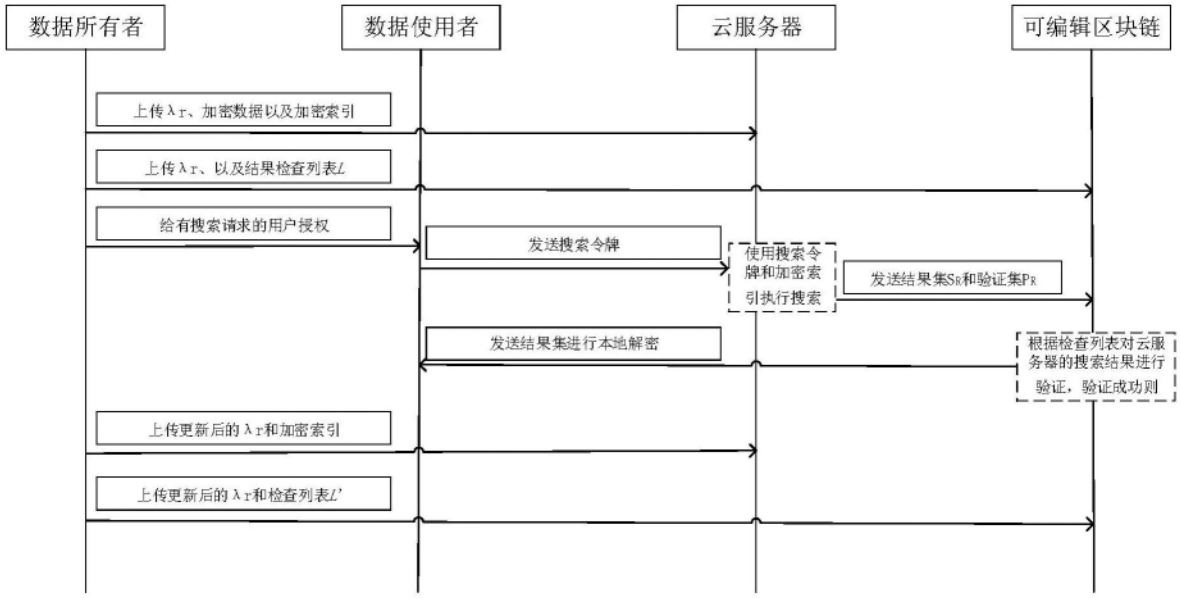

数据所有者
数据使用者
云服务器
可编辑区块链
上传λT、加密数据以及加密索引
上传λT、以及结果检查列表L
给有搜索请求的用户授权
发送搜索令牌
使用搜索令牌和加密索引执行搜索
发送结果集SR和验证集PR
发送结果集进行本地解密
根据检查列表对云服务器的搜索结果进行验证，验证成功则
上传更新后的λT和加密索引
上传更新后的λT和检查列表L'

图4

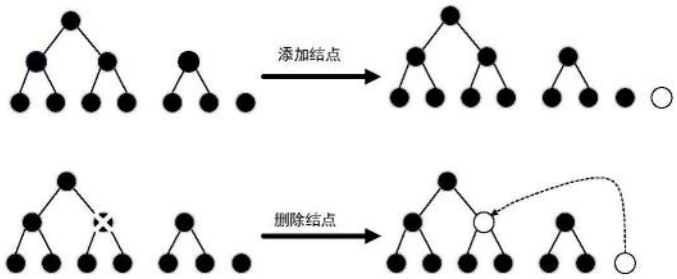


图5

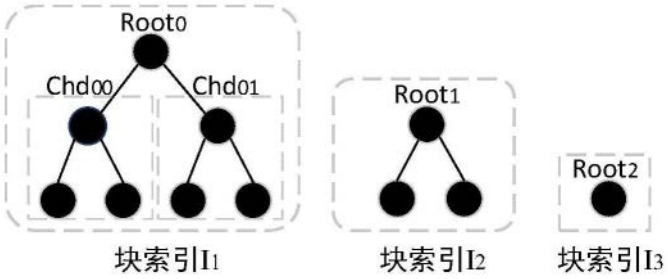


图6