(19)中华人民共和国国家知识产权局

(12)发明专利申请

(10)申请公布号 CN 114124499 A
(43)申请公布日 2022.03.01

(21)申请号 202111344485.2

(22)申请日 2021.11.15

(71)申请人 中国科学院沈阳计算技术研究所有限公司
地址 110168 辽宁省沈阳市东陵区南屏东路16号

(72)发明人 于金刚 温直锋 于波 侯勇康 于碧辉 李姝

(74)专利代理机构 沈阳科苑专利商标代理有限公司 21002
代理人 王倩

(51)Int.Cl.
H04L 9/40(2022.01)
H04L 9/06(2006.01)

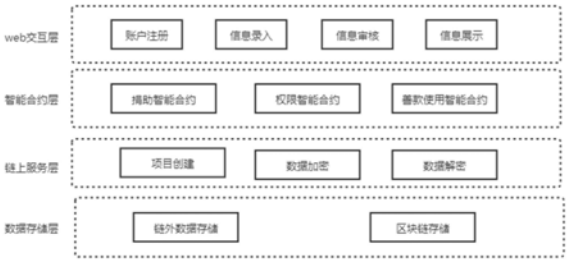
权利要求书2页 说明书6页 附图4页

(54)发明名称

基于区块链的慈善系统隐私保护方法与系统

(57)摘要

本发明涉及基于区块链的慈善系统隐私保护方法与系统。提出将本慈善系统隐私保护分为面向用户的隐私保护和面向数据的隐私保护。面向用户的隐私保护通过编写智能合约,限制用户访问数据权限,保证隐私数据;面向数据的隐私保护通过使用改进的AES算法,动态构造S盒,使其各种性质呈随机变换的特性,增加加密算法的安全性;同时使用摘要算法,对生成的密文计算摘要,保证数据的完整性。使用改进的AES算法和摘要算法在保证慈善系统中数据加密安全性和完整性的同时,提升了运行效率,从而使整个系统具有足够的公信力,有效地弥补了传统慈善系统数据泄露的风险。



CN 114124499 A

1.基于区块链的慈善系统隐私保护方法,其特征在于,包括以下步骤:

根据智能合约限制慈善系统中用户的访问权限;

对上传区块链的信息进行基于动态构造S盒的AES算法加密并存储。

2.根据权利要求1所述的基于区块链的慈善系统隐私保护方法,其特征在于,所述基于动态构造S盒的AES算法,包括以下步骤:

步骤1:对提供的密钥key进行Murmurhash2变换,计算出32bit变换因子E,转换成十六进制数共八位,将其分为高四位和低四位:

E=Murmurhash2(key)

其中,Murmurhash2表示Murmurhash2变换,key表示AES算法的加密密钥;

步骤2:将高四位h和第四位1分别添加不同的干扰因子(u,v),分别作为行和列的变换变量(k,p);干扰因子从素数F{X_1,x_2,…x_n}集合中选择;

k=(h+u)mod 16 u∈rondom(F)

p=(l+v)mod16 v∈rondom(F)

其中,mod表示取余,rondom表示从素数集合F中随机选取一个数;

步骤3:初始化一个16×16的S盒矩阵,矩阵中元素的值从0开始,依次递增,直到255,逐行从左至右填入矩阵的256个位置,表示为T_0;

步骤4:对初始S盒矩阵,遍历每一行数据,首先进行行变换,然后将T_0中i、j位置元素值赋值给对应的T_1的x、j位置元素值;公式如下:

x=(k+i+j)mod 16

$T_1[x][j]=T_0[i][j]$

其中,i、j分别表示当前数据在S盒T_0中的行、列坐标,k表示行变换变量,x表示最终行移动的位数,T_1表示临时存储矩阵;

步骤5:对行变换生成的矩阵T_1进行列变换,将T_1中i、j位置对应值赋值给T_2的i、y位置;公式如下:

y=(p+i+j)mod 16

$T_2[i][y]=T_1[i][j]$

其中,i、j表示T_1矩阵中的行、列坐标,p表示列变换变量,y表示最终列移动的位数,T_2表示临时存储矩阵;

得到的T_2矩阵即为生成的S盒;

步骤6:根据生成的S盒,通过位置交换得到逆S盒;

步骤7:将明文拆成多个独立的明文块,每个明文块的长度是128bit;当明文块少于128bit时,则在明文块末尾补足空字符,以使该明文块长度为128bit;

步骤8:将AES算法的字节代替过程中的S盒替换为步骤5生成的S盒,对每个明文块执行AES算法,并将生成的密文块进行拼接,生成完整的密文。

3.根据权利要求2所述的基于区块链的慈善系统隐私保护方法,其特征在于,所述干扰因子为常数,分别作为行变换变量K和列变换变量P。

4.根据权利要求2所述的基于区块链的慈善系统隐私保护方法,其特征在于,所述根据生成的S盒,通过位置交换得到逆S盒,包括以下步骤:

初始一个16×16的矩阵S_1,每个位置的值为0;

S盒的i行、j列位置的数据，表现为0xmn，在S_1矩阵的m行，n列位置填入0xij，形成对应；

遍历S盒中所有元素，依次将S_1矩阵填充完成，得到的S_1为逆S盒。

5.根据权利要求2所述的基于区块链的慈善系统隐私保护方法，其特征在于，对权利要求2所述生成的密文通过使用SHA256算法对密文计算摘要，将计算结果拼接到密文后面，用于验证密文的完整性。

6.根据权利要求2或4所述的基于区块链的慈善系统隐私保护方法，其特征在于，对加密后的上传区块链的信息进行解密，通过构建的逆S盒进行解密。

7.根据权利要求1所述的基于区块链的慈善系统隐私保护方法，其特征在于，所述上传区块链的信息包括：受助信息、捐助信息以及账户使用信息。

8.根据权利要求1所述的基于区块链的慈善系统隐私保护方法，其特征在于，所述智能合约层设置受助者访问权限、捐助者访问权限以及监督者访问权限；

所述受助者访问权限：访问受助信息，包括总共捐款金额，以及捐助人的捐款金额，无权访问捐助人的个人信息；

所述捐助者访问权限：访问本人参与的捐助信息，受助人的受助信息，以及受助人的善款使用信息，无权访问受助人的个人信息；

所述监督者使用权限：访问所有的受助信息，所有捐助人的捐助信息，以及所有善款的使用信息。

9.基于区块链的慈善系统隐私保护系统，其特征在于，包括：

应用层，用于区块链慈善系统与外部信息交互，将信息传入智能合约层；

智能合约层，用于将传入信息编写成智能合约，以限制用户的访问权限；

数据处理层，用于将上传至区块链中的信息进行加密。

基于区块链的慈善系统隐私保护方法与系统

技术领域

[0001] 本发明涉及到了区块链技术以及密码学数据加密和解密领域，总结起来就是基于区块链的慈善系统隐私保护的方法与系统。

背景技术

[0002] 在慈善领域内，通过区块链技术的先进的特点，通过网上募捐等手段，记录善款的流动方向，随时可以查询善款的去向。应用区块链技术的慈善系统可以做到善款追踪，对于慈善账目进行公正公开等操作，提升慈善组织对于信息的透明度，从而实现公众对于慈善组织的信任感的提升。

[0003] 在保证慈善系统公信力的同时，更需要注重用户的隐私数据。数据的自身价值在信息化的今天不断凸显，如何保证核心数据的安全，是一个重大的挑战。对于用户而言，用户期望自己的数据得到保护。所以在保证数据高效可用的同时，如何进行数据的隐私保护，成为当前国内外科研人员研究的热点之一。

[0004] 区块链作为一项新技术，与传统的IT架构存在明显的区别。在传统的IT架构中，数据通常保存在中心化服务器，如何保证数据的隐私安全转变为如何保证中心服务器的安全，通过购买高性能的服务器或者提高服务器的抗攻击能力是隐私保护的重点。但是对于区块链系统的隐私保护始终没有合适的解决方案。区块链作为多个节点共同参与监督和管理的分布式数据库系统，已经成为互联网发展的趋势。

[0005] 目前主流的加密算法有，同态加密，安全多方计算，以及密钥管理等。同态加密是实现第三方在不解密的情况下对数据进行计算和验证，安全多方计算式一种通用的密码原语，是互不信任的分布式环境下多个数据所有者，联合计算同一函数，而不泄露自己的输入数据。密钥管理是按照是否访问互联网划分，冷钱包不能被网络访问，避免了黑客盗取私钥的风险。热钱包在联网的状态下，可以随时进行交易，对于频繁交易的用户来说，热钱包会更加便捷。

[0006] 如何保证区块链上用户隐私数据不被窃取，是主要研究的工作重点。现有的隐私保护方法主要是使用非对称加密算法对数据加密。通过公钥加密信息，使用私钥进行解密，或者使用私钥加密信息，通过公钥解密。该方法加密和解密都要花费大量的时间，速度慢，只适合对少量数据进行加密。但对于慈善系统产生的大量数据而言，并不适用。

发明内容

[0007] 为了满足慈善系统公开性、透明性、不可篡改性和数据安全性的需求，本发明提供一种基于区块链的慈善系统隐私保护方法与系统。该系统重点解决隐私保护问题。采用了面向用户以及面向数据的隐私保护方法。本发明通过使用区块链智能合约以及密码学相关知识解决隐私保护问题。对于用户，通过编写智能合约，控制用户的访问权限，保证用户隐私数据。对于数据，利用加密算法对数据进行加密，同时使用摘要算法进行完整性校验，提高数据安全性。针对数据加密问题，研究人员提出了了多种加密算法。本文主要针对AES算

法进行改进，通过动态构造S盒，使其不具有明显的结构特点，各种性质呈随机变换的特性，增加了破解的难度；同时使用摘要算法，保证用户数据的完整性。最后，验证数据加密的运行效率，验证改进算法的正确性和可行性。

[0008] 本发明为实现上述目的所采用的技术方案是：基于区块链的慈善系统隐私保护方法，包括以下步骤：

[0009] 根据智能合约限制慈善系统中用户的访问权限；

[0010] 对上传区块链的信息进行基于动态构造S盒的AES算法加密并存储。

[0011] 所述基于动态构造S盒的AES算法，包括以下步骤：

[0012] 步骤1：对提供的密钥key进行Murmurhash2变换，计算出32bit变换因子E，转换成十六进制数共八位，将其分为高四位和低四位：

[0013] E＝Murmurhash2(key)

[0014] 其中，Murmurhash2表示Murmurhash2变换，key表示AES算法的加密密钥；

[0015] 步骤2：将高四位h和第四位1分别添加不同的干扰因子(u,v)，分别作为行和列的变换变量(k,p)；干扰因子从素数F$\{x_1,x_2,\cdots x_n\}$集合中选择；

[0016] k＝(h+u)mod 16u∈rondom(F)

[0017] p＝(l+v)mod16v∈rondom(F)

[0018] 其中，mod表示取余，rondom表示从素数集合F中随机选取一个数；

[0019] 步骤3：初始化一个16×16的S盒矩阵，矩阵中元素的值从0开始，依次递增，直到255，逐行从左至右填入矩阵的256个位置，表示为T_0；

[0020] 步骤4：对初始S盒矩阵，遍历每一行数据，首先进行行变换，然后将T_0中i、j位置元素值赋值给对应的T_1的x、j位置元素值；公式如下：

[0021] x＝(k+i+j)mod 16

[0022] $T_1[x][j]=T_0[i][j]$

[0023] 其中，i、j分别表示当前数据在S盒T_0中的行、列坐标，k表示行变换变量，x表示最终行移动的位数，T_1表示临时存储矩阵；

[0024] 步骤5：对行变换生成的矩阵T_1进行列变换，将T_1中i、j位置对应值赋值给T_2的i、y位置；公式如下：

[0025] y＝(p+i+j)mod 16

[0026] $T_2[i][y]=T_1[i][j]$

[0027] 其中，i、j表示T_1矩阵中的行、列坐标，p表示列变换变量，y表示最终列移动的位数，T_2表示临时存储矩阵；

[0028] 得到的T_2矩阵即为生成的S盒；

[0029] 步骤6：根据生成的S盒，通过位置交换得到逆S盒；

[0030] 步骤7：将明文拆成多个独立的明文块，每个明文块的长度是128bit；当明文块少于128bit时，则在明文块末尾补足空字符，以使该明文块长度为128bit；

[0031] 步骤8：将AES算法的字节代替过程中的S盒替换为步骤5生成的S盒，对每个明文块执行AES算法，并将生成的密文块进行拼接，生成完整的密文。

[0032] 所述干扰因子为常数，分别作为行变换变量K和列变换变量P。

[0033] 所述根据生成的S盒，通过位置交换得到逆S盒，包括以下步骤：

[0034] 初始一个16×16的矩阵S_1,每个位置的值为0;

[0035] S盒的i行、j列位置的数据,表现为0xmn,在S_1矩阵的m行,n列位置填入0xij,形成对应;

[0036] 遍历S盒中所有元素,依次将S_1矩阵填充完成,得到的S_1为逆S盒。

[0037] 对生成的密文通过使用SHA256算法对密文计算摘要,将计算结果拼接到密文后面,用于验证密文的完整性。

[0038] 对加密后的上传区块链的信息进行解密,通过构建的逆S盒进行解密。

[0039] 所述上传区块链的信息包括:受助信息、捐助信息以及账户使用信息。

[0040] 所述智能合约层设置受助者访问权限、捐助者访问权限以及监督者访问权限;

[0041] 所述受助者访问权限:访问受助信息,包括总共捐款金额,以及捐助人的捐款金额,无权访问捐助人的个人信息;

[0042] 所述捐助者访问权限:访问本人参与的捐助信息,受助人的受助信息,以及受助人的善款使用信息,无权访问受助人的个人信息;

[0043] 所述监督者使用权限:访问所有的受助信息,所有捐助人的捐助信息,以及所有善款的使用信息。

[0044] 基于区块链的慈善系统隐私保护系统,包括:

[0045] 应用层,用于区块链慈善系统与外部信息交互,将信息传入智能合约层;

[0046] 智能合约层,用于将传入信息编写成智能合约,以限制用户的访问权限;

[0047] 数据处理层,用于将上传至区块链中的信息进行加密。

[0048] 本发明具有以下有益效果及优点:

[0049] 1.本发明相对于现有慈善系统,具有更高的隐私保护要求和极高的可信度。

[0050] 2.对慈善系统的数据访问设置用户访问权限,不同的用户有不同的访问权限,从用户角度提供隐私保护。

[0051] 3.通过动态构造S盒,使用AES算法进行加密,来保证用户的隐私数据。经过使用改进的AES算法加密之后,存储在区块链,从数据角度保护隐私安全。

[0052] 4.对交易产生的数据经过加密算法加密之后,计算摘要,保证数据完整性。

[0053] 5.对慈善系统采用链上链下相结合的方式,提供区块链的空间利用率。

附图说明

[0054] 图1为本发明面向用户的隐私保护模型示意图;

[0055] 图2为本发明面向数据的隐私保护模型示意图;

[0056] 图3a为生成的S盒示意图;

[0057] 图3b为生成的逆S盒示意图;

[0058] 图4为该慈善系统捐助和查询流程图;

[0059] 图5为基于区块链的慈善系统隐私保护系统示意图。

具体实施方式

[0060] 下面结合附图及实施例对本发明做进一步的详细说明。

[0061] 本发明面向用户的隐私保护通过编写智能合约,限制用户访问数据权限,保证隐

私数据;面向数据的隐私保护通过使用改进的AES算法,动态构造S盒,使其各种性质呈随机变换的特性,增加加密算法的安全性;同时使用摘要算法,对生成的密文计算摘要,保证数据的完整性。使用改进的AES算法和摘要算法在保证慈善系统中数据加密安全性和完整性的同时,提升了运行效率,从而使整个系统具有足够的公信力,有效地弥补了传统慈善系统数据泄露的风险。

[0062] 如图5所示,基于区块链的慈善系统隐私保护的系统包括:

[0063] 应用层:用于区块链慈善系统与外部信息交互,将信息传入智能合约层;

[0064] 智能合约层,用于将传入信息编写成智能合约,以限制用户的访问权限;

[0065] 数据处理层,用于将上传至区块链中的信息进行加密和解密;

[0066] 数据存储层:用于存储用户及系统产生的数据信息。

[0067] 通过编写权限智能合约限制用户的访问权限,保证用户的隐私数据。

[0068] 通过对写入区块链的数据进行加密,使用改进的AES算法,动态构造S盒,使其不具有明显的结构特点,增加了破解难度,同时改进摘要算法,保证用户数据的完整性。

[0069] 交互信息包括:受助者提供的受助信息、捐助信息以及善款的使用信息。

[0070] 智能合约层包括:受助者访问权限、捐助者访问权限以及监督者访问权限。

[0071] 受助者访问权限:访问受助相关的信息,包括总共捐款金额,以及捐助人的捐款金额,无权访问捐助人的个人信息。

[0072] 捐助者访问权限:访问该用户参与的捐助记录,受助人的受助信息,以及受助人的善款使用记录,无权访问受助人的个人信息。

[0073] 监督者使用权限:访问所有的受助信息,所有捐助人的捐助记录,以及所有善款的使用记录。

[0074] 所述数据存储层包括:链下存储模块和链上存储模块。

[0075] 链下存储模块:采用传统数据库存储,保存用户的基本信息,包括用户的账户、角色以及用户唯一标识ID。

[0076] 链上存储模块:采用区块链存储,保存慈善系统相关数据,包括受助人的受助申请、捐助人的捐款记录以及善款使用记录。

[0077] 数据保护采用改进的AES算法和摘要算法,包括动态构造S盒、将AES算法并行化以及对加密数据计算摘要。

[0078] 动态构造S盒:通过对密钥进行Murmurhash2变换,同时添加干扰因子,对初始化的S盒进行旋转,使其不具有明显的结构特点,各种性质呈随机变换的特性,不同的密钥生成不同的S盒,保证信息安全。

[0079] AES算法并行化:传统的AES算法为串行结构,会导致系统加密解时间响应过长,交互体验变差等问题。为此,可将AES算法的串行化结构改为并行化计算结构,如图2所示,可提高数据加解密的计算效率。

[0080] 计算摘要:通过对加密后的密文计算摘要,保证密文前后一致性、数据完整性。

[0081] 受助者将受助信息提交给监督者审核,审核通过后,将受助信息上传至区块链。捐助者通过选择受助项目进行捐助。具体包括以下步骤:

[0082] 区块链慈善系统将受助者提交的信息由监督者审核通过后,传入智能合约层;

[0083] 智能合约层根据提交的受助信息,生存对应的智能合约;

[0084] 数据处理层对登记的受助信息进行记录，并对交互数据进行加密；

[0085] 数据存储层对加密后的数据进行存储。

[0086] 如图1所示，本文所设计的基于区块链的慈善系统隐私保护主要分为两部分，其具体内容如下：

[0087] (1)面向用户的隐私保护

[0088] 面向用户的隐私保护是用户对数据的访问控制权限以及在区块链系统中的匿名性，访问控制策略是数据隐私保护的重要策略之一，通过限制数据的访问权限，信息不会被非法获取，从而保证数据安全。

[0089] 在慈善系统中，用户通过注册申请，系统管理员通过审核信息，为用户分配角色。用户获得角色权限后，可在权限范围，通过系统中的智能合约，确定访问的信息。如果用户没有访问权限，则无法查询对应的数据。整个慈善系统包括一下几个角色：

[0090] 普通用户角色：包括受捐者和捐助者，可以访问与之相关的捐助受助信息。

[0091] 系统管理者：为用户分配角色，确定不同用户的访问权限。

[0092] 监督者：根据智能合约的编写规则，验证用户是否具有访问权限，如果具有访问权限，则通过区块链账户获取相关信息，返回给用户。

[0093] 其中智能合约主要针对系统用户设定访问规则，每个用户包含的用户权限。系统管理者可以根据智能合约的规则，分配不同的用户权限，提高智能合约的灵活度。

[0094] (2)面向数据的隐私保护

[0095] 面向数据的隐私保护主要是面向数据信息本身，主要是采用基于加密的隐私保护方法，保护数据的隐私性和完整性。慈善系统中的用户上传到区块链的信息可能包含一部分隐私信息，为防止其他攻击者非法获取用户数据，必须对上链信息进行加密。为兼顾加密安全和加密效率，本文在AES算法的基础上，改进了S盒的生成过程，增加破译信息的难度，同时使用摘要算法验证信息的完整性，保证信息安全。

[0096] 如图2所示，具体步骤为：

[0097] 步骤1：先对提供的密钥key进行Murmurhash2变换，计算出32bit变换因子E，将其分为高四位和低四位。

[0098] E＝Murmurhash2(key)

[0099] 步骤2：将高四位h和第四位1分别添加不同的干扰因子(u,v)，该干扰因子可以从素数F$\{x_1,x_2,\cdots x_n\}$集合中选择。也可以为一个常数值，分别作为行变换变量K和列变换变量P。

[0100] k＝(h+u)mod16u∈rondom(F)

[0101] p＝(l+v)mod16v∈rondom(F)

[0102] 步骤3：初始化一个16×16的S盒矩阵，矩阵的值从小到大依次为0～255，每一行从小到大排列，依次填入矩阵的对应位置，表示为T_0。

[0103] 步骤4：对初始S盒矩阵，遍历每一行数据，首先进行行变换，变换公式如下：

[0104] x＝(k+i+j)mod 16

[0105] $T_1[x][i]=T_0[j][i]$

[0106] 其中，i，j表示当前数据在S盒T_0中的行、列坐标，k表示行变换变量，x表示最终行移动的位数，T_1表示临时存储矩阵。然后将T_0中j、i位置对应位置赋值给T_1的x，i位置。

[0107] 步骤5:对行变换生成的矩阵T_1进行列变换,变换公式如下:

[0108] $y=(p+i+j) \bmod 16$

[0109] $T_2[i][y]=T_1[i][j]$

[0110] 其中i、j表示T_1矩阵中的行、列坐标,p表示列变换变量,y表示最终列移动的位数,T_2表示临时存储矩阵。将T_1中i,j位置对应值赋值给T_2的i,y位置。取h和l分别为3,5,u、v为2,3,生成的S盒T_2如下图3a、图3b:

[0111] 步骤6:根据生成的S矩阵,将对应位置进行交换。如图3a、图3b,取S盒0行,0列位置的数据为2e,在逆S盒中2行,e列的对应位置为00,依次将矩阵填充完成,结果为逆S盒,不需要再次计算。

[0112] 步骤7:将明文拆成一个个独立的明文块,每个明文块的长度是128bit,如果明文块少于128bit,则在明文块末尾补足相应数量的空字符。

[0113] 步骤8:对每个明文块执行AES算法的字节代替、行移位、列混淆以及轮密钥加操作,将字节代替过程中的S盒替换为改进的S盒。最终生成的密文块进行拼接,生成完整的密文块。

[0114] 对生成的密文通过使用SHA256摘要算法对密文计算摘要,将计算结果拼接到密文后面,用于验证密文的完整性。

[0115] 如图4,本发明包括以下步骤:

[0116] 1.受助人提供受助信息,生成智能合约。受助人通过填写基本的受助信息,包括受助原因、金额、凭证以及基本情况等,将信息提交给监督者,监督者审核通过后,生成智能合约,发布到区块链上。

[0117] 2.捐助人查询受助信息,进行捐助。捐助人登录系统后,可以查询受助人提供的受助信息,通过向指定的监管账户进行转账,对受助进行捐助。

[0118] 3.捐助信息加密后存储在区块链中。捐助人捐助之后,将转账凭证在系统中提交,由监督者审核通过后,对数据进行加密,存储在区块链中。

[0119] 4.监督者监督善款账户动态,将信息记录在区块链中。在捐助结束之后,受助人可以使用监管账户中的善款,将使用善款的凭证由监督者保存在区块链中。

[0120] 5.受助人和捐助人查询相关信息。受助人可以在任何时间查询善款捐助情况,同时捐助可以查询自己所有的捐款记录和善款使用情况,但是对于超出其权限范围的其他信息,无权访问。

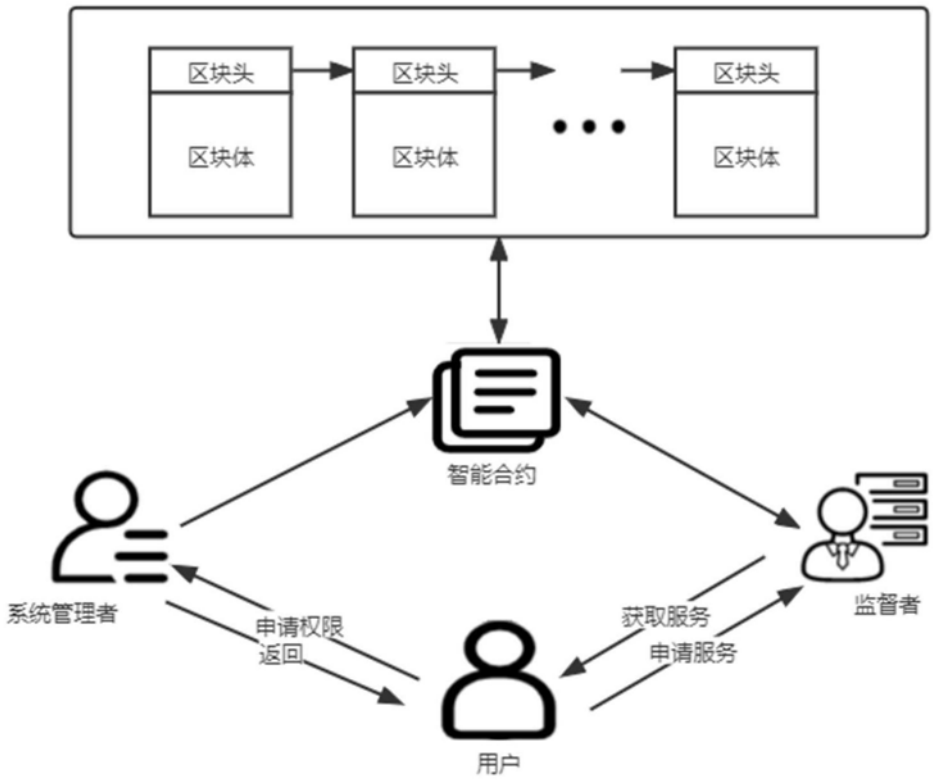


图1

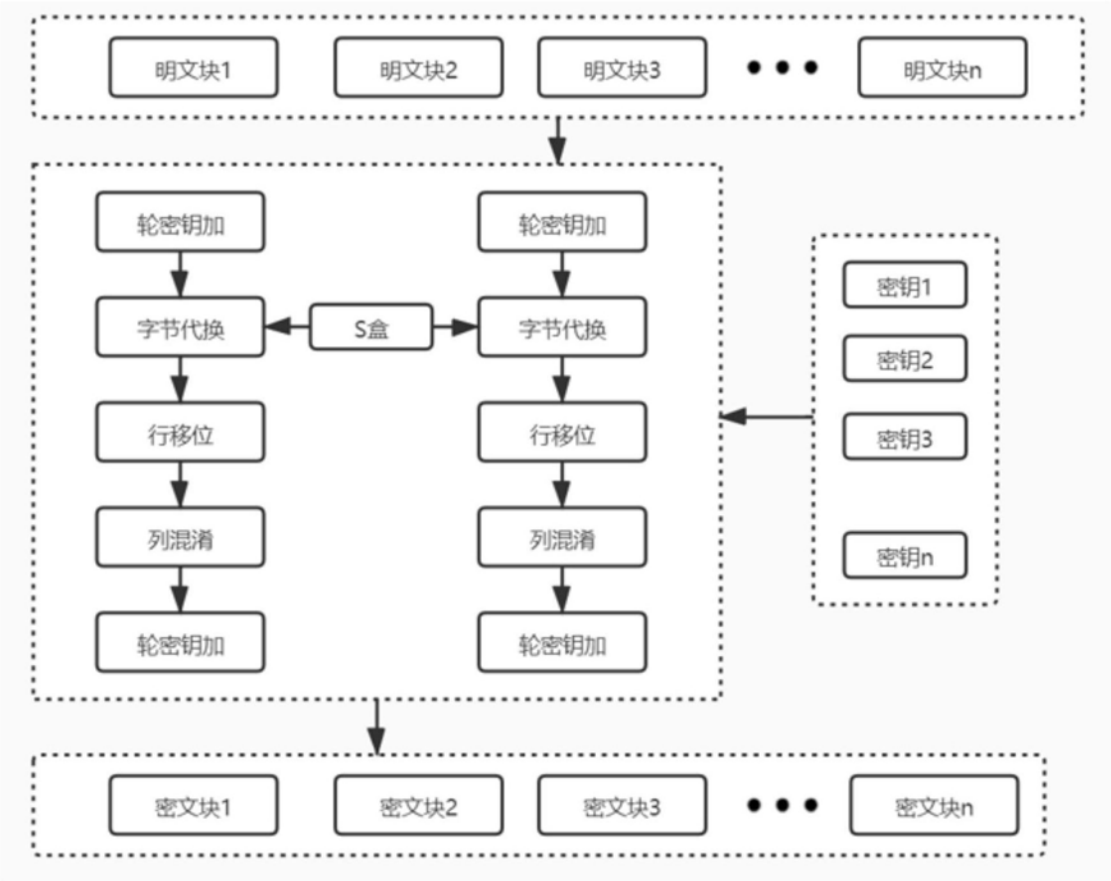


图2

[2e 10 02 f4 e6 d8 ca bc ae 90 82 74 66 58 4a 3c]
[52 60 7e 8c 9a a8 b6 c4 d2 e0 fe 0c 1a 28 36 44]
[00 f2 e4 d6 c8 ba ac 9e 80 72 64 56 48 3a 2c 1e]
[70 8e 9c aa b8 c6 d4 e2 f0 0e 1c 2a 38 46 54 62]
[6a 5c 4e 30 22 14 06 f8 ea dc ce b0 a2 94 86 78]
[e9 f7 05 13 21 3f 4d 5b 69 77 85 93 a1 bf cd db]
[4c 3e 20 12 04 f6 e8 da cc be a0 92 84 76 68 5a]
[cb d9 e7 f5 03 11 2f 3d 4b 59 67 75 83 91 af bd]
[b5 a7 99 8b 7d 6f 51 43 35 27 19 0b fd ef d1 c3]
[25 33 41 5f 6d 7b 89 97 a5 b3 c1 df ed fb 09 17]
[d3 c5 b7 a9 9b 8d 7f 61 53 45 37 29 1b 0d ff e1]
[07 15 23 31 4f 5d 6b 79 87 95 a3 b1 cf dd eb f9]
[f1 e3 d5 c7 b9 ab 9d 8f 71 63 55 47 39 2b 1d 0f]
[16 24 32 40 5e 6c 7a 88 96 a4 b2 c0 de ec fa 08]
[1f 01 f3 e5 d7 c9 bb ad 9f 81 73 65 57 49 3b 2d]
[34 42 50 6e 7c 8a 98 a6 b4 c2 d0 ee fc 0a 18 26]

图3a

[20 e1 02 74 64 52 46 b0 df 9e fd 8b 1b ad 39 cf]
[01 75 63 53 45 b1 d0 9f fe 8a 1c ac 3a ce 2f e0]
[62 54 44 b2 d1 90 ff 89 1d ab 3b cd 2e ef 00 76]
[43 b3 d2 91 f0 88 1e aa 3c cc 2d ee 0f 77 61 55]
[d3 92 f1 87 1f a9 3d cb 2c ed 0e 78 60 56 42 b4]
[f2 86 10 a8 3e ca 2b ec 0d 79 6f 57 41 b5 d4 93]
[11 a7 3f c9 2a eb 0c 7a 6e 58 40 b6 d5 94 f3 85]
[30 c8 29 ea 0b 7b 6d 59 4f b7 d6 95 f4 84 12 a6]
[28 e9 0a 7c 6c 5a 4e b8 d7 96 f5 83 13 a5 31 c7]
[09 7d 6b 5b 4d b9 d8 97 f6 82 14 a4 32 c6 27 e8]
[6a 5c 4c ba d9 98 f7 81 15 a3 33 c5 26 e7 08 7e]
[4b bb da 99 f8 80 16 a2 34 c4 25 e6 07 7f 69 5d]
[db 9a f9 8f 17 a1 35 c3 24 e5 06 70 68 5e 4a bc]
[fa 8e 18 a0 36 c2 23 e4 05 71 67 5f 49 bd dc 9b]
[19 af 37 c1 22 e3 04 72 66 50 48 be dd 9c fb 8d]
[38 c0 21 e2 03 73 65 51 47 bf de 9d fc 8c 1a ae]

图3b

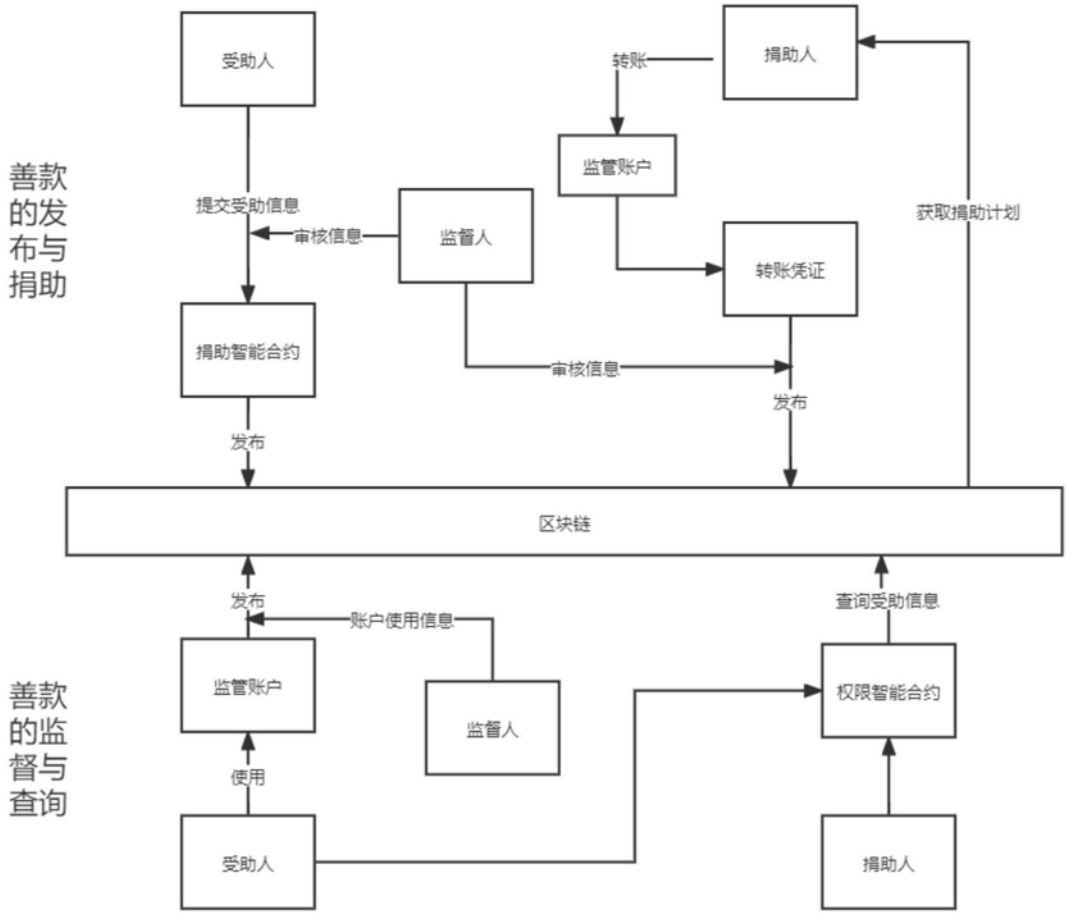


图4

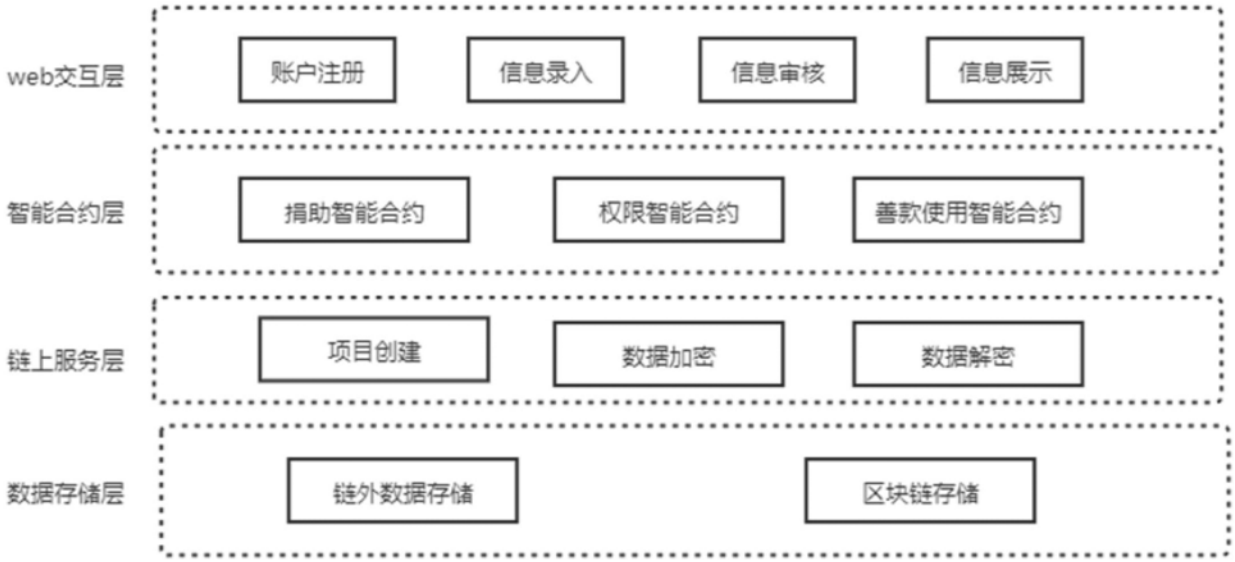

web交互层
账户注册
信息录入
信息审核
信息展示
智能合约层
捐助智能合约
权限智能合约
善款使用智能合约
链上服务层
项目创建
数据加密
数据解密
数据存储层
链外数据存储
区块链存储

图5