(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 108881240 B
(45)授权公告日 2021.04.30

(21)申请号 201810668555.1

(22)申请日 2018.06.26

(65)同一申请的已公布的文献号
申请公布号 CN 108881240 A

(43)申请公布日 2018.11.23

(73)专利权人 广州天高软件科技有限公司
地址 510000 广东省广州市越秀区东风东路733(1)号自编7楼711房(仅限办公用途)

(72)发明人 金风莲

(74)专利代理机构 成都行之专利代理事务所(普通合伙) 51220
代理人 宋辉

(51)Int.Cl.
H04L 29/06(2006.01)
H04L 29/08(2006.01)

(56)对比文件
CN 106503574 A,2017.03.15
CN 107171785 A,2017.09.15
CN 107203344 A,2017.09.26
EP 3525389 A1,2019.08.14

审查员 周天豪

权利要求书1页 说明书4页

(54)发明名称

基于区块链的会员隐私数据保护方法

(57)摘要

本发明公开了基于区块链的会员隐私数据保护方法,采用上述方法,使用私钥对会员数据进行加密,私钥掌握在会员自己手中,需要查询会员的数据存储节点上的会员数据时,需要使用会员手中的私钥对数据进行解密,因此,任何人查看会员数据都需要经过用户的同意,而写入数据由于不涉及隐私问题,如果每次数据写入都需要会员确认较为不便,因此本系统不需要用户确认也可写入数据。解决用户隐私得不到有效保障;用户的共享需求通过共享处理中心,一旦因某种原因而导致共享处理中心无法工作,便无法实现数据共享的问题。

CN 108881240 B

1.基于区块链的会员隐私数据保护方法,其特征在于,包括以下步骤:

A、为每个会员匹配一个数据储存节点;

B、为每个数据存储节点匹配一个私钥,将私钥发送给对应的会员;

C、根据步骤B中匹配的所有私钥生成对应的公钥,将公钥在全网广播;

D、建立用户终端节点,为用户终端节点匹配一个密匙,将与密匙匹配的密钥发送给会员系统的所有者;

还包括数据写入的步骤:

E、会员系统的所有者通过密钥进入用户终端节点;

F、用户终端节点提取需要写入信息的会员的公钥,将需要写入的信息通过公钥进行加密;

G、用户终端节点发起请求,请求为对应会员的数据存储节点创建一个新的数据区块,将加密后的需要写入的信息存储在新的数据区块中;

H、各节点通过共识机制校验达成步骤G中请求的合法性验证,通过校验后,新的数据区块添加至对应会员的数据存储节点上;

还包括数据读取的步骤:

J、会员系统的所有者通过密钥进入用户终端节点;

K、用户终端节点发起请求,请求读取指定会员的数据;

L、各节点通过共识机制校验达成步骤K中请求的合法性验证,通过校验后,对应会员的数据储存节点上连接的数据区块中的数据均发送到用户终端节点;

I、对应的会员使用手中的私钥对数据区块中的数据进行解密,获取对应的会员数据。

2.根据权利要求1所述的基于区块链的会员隐私数据保护方法,其特征在于,所述步骤C中根据步骤B中匹配的所有私钥生成对应的公钥的方法采用RSA公钥系统或椭圆曲线密码系统中的一种。

3.根据权利要求1所述的基于区块链的会员隐私数据保护方法,其特征在于,所述步骤H中的共识机制为由用户终端节点完成校验。

4.根据权利要求1所述的基于区块链的会员隐私数据保护方法,其特征在于,所述步骤L中的共识机制为由指定会员的数据储存节点完成校验。

基于区块链的会员隐私数据保护方法

技术领域

[0001] 本发明涉及一种数据包括方法,具体涉及基于区块链的会员隐私数据保护方法。

背景技术

[0002] 区块链是一种分布式数据存储方案,其通过点对点模式提供一种去中心化方式的集体维 护策略。该技术将一段时间内的系统交流数据汇总,通过现代密码学手段把汇总数据生成数 据区块,并利用时间戳产生数据指纹,将数据区块串联成链并提供有效性验证和审计。

[0003] 传统的用户数据存储及共享方法主要有两种:集中存储集中共享和分布式存储集中共享。集中存储集中共享的工作过程为:服务方采集所有用户的数据并集中存储,每一个共享请求 都要发送到服务器中心进行审核处理;分布式存储集中共享的工作过程为:服务器采集所有 用户数据并通过分布式技术分散存储,当用户发起共享请求时,通过服务中心审核处理。第 一种方法采用集中存储方式,维护方便,安全性高,但由于工作量较大容易产生服务瓶颈; 第二种方法采用分布式存储技术,但共享需求依然通过中心服务器处理,当处理时还要通过 分布式存储寻找所需数据,增加了系统复杂度。另外,两种方式存储的数据虽都经过加密处 理,但作为服务方依然可以自由利用,用户隐私得不到有效保障;用户的共享需求通过共享 处理中心,一旦因某种原因而导致共享处理中心无法工作,便无法实现数据共享。

发明内容

[0004] 本发明所要解决的技术问题是用户隐私得不到有效保障;用户的共享需求通过共享处理 中心,一旦因某种原因而导致共享处理中心无法工作,便无法实现数据共享,目的在于提供 基于区块链的会员隐私数据保护方法,解决用户隐私得不到有效保障;用户的共享需求通过 共享处理中心,一旦因某种原因而导致共享处理中心无法工作,便无法实现数据共享的问题。

[0005] 本发明通过下述技术方案实现:

[0006] 基于区块链的会员隐私数据保护方法,包括以下步骤:

[0007] A、为每个会员匹配一个数据储存节点;

[0008] B、为每个数据存储节点匹配一个私钥,将私钥发送给对应的会员;

[0009] C、根据步骤B中匹配的所有私钥生成对应的公钥,将公钥在全网广播;

[0010] D、建立用户终端节点,为用户终端节点匹配一个密匙,将与密匙匹配的密钥发送给会 员系统的所有者;

[0011] 还包括数据写入的步骤:

[0012] E、会员系统的所有者通过秘钥进入用户终端节点;

[0013] F、用户终端节点提取需要写入信息的会员的公钥,将需要写入的信息通过公钥进行加密;

[0014] G、用户终端节点发起请求，请求为对应会员的数据存储节点创建一个新的数据区块，将加密后的需要写入的信息存储在新的数据区块中；

[0015] H、各节点通过共识机制校验达成步骤G中请求的合法性验证，通过校验后，新的数据 区块添加至对应会员的数据存储节点上；

[0016] 还包括数据读取的步骤：

[0017] J、会员系统的所有者通过秘钥进入用户终端节点；

[0018] K、用户终端节点发起请求，请求读取指定会员的数据；

[0019] L、各节点通过共识机制校验达成步骤K中请求的合法性验证，通过校验后，对应会员 的数据储存节点上连接的数据区块中的数据均发送到用户终端节点；

[0020] I、对应的会员使用手中的私钥对数据区块中的数据进行解密，获取对应的会员数据。

[0021] 采用上述方法，使用私钥对会员数据进行加密，私钥掌握在会员自己手中，需要查询会 员的数据存储节点上的会员数据时，需要使用会员手中的私钥对数据进行解密，因此，任何 人查看会员数据都需要经过用户的同意，而写入数据由于不涉及隐私问题，如果每次数据写 入都需要会员确认较为不便，因此本系统不需要用户确认也可写入数据。

[0022] 所述步骤C中根据步骤B中匹配的所有私钥生成对应的公钥的方法采用RSA公钥系统 或椭圆曲线密码系统中的一种。

[0023] 所述步骤H中的共识机制为由用户终端节点完成校验。由于会员数据的写入有时涉及会 员系统所有者的权益，因此，写入时的共识机制为用户终端节点完成校验。

[0024] 所述步骤L中的共识机制为由指定会员的数据储存节点完成校验。由于会员数据的读取 涉及会员的权益，因此，读取时的共识机制为指定会员的数据储存节点完成校验。

[0025] 本发明与现有技术相比，具有如下的优点和有益效果：

[0026] 1、本发明基于区块链的会员隐私数据保护方法，区块链系统较为简单，便于搭建；

[0027] 2、本发明基于区块链的会员隐私数据保护方法，能有效的保护会员的隐私数据；

[0028] 3、本发明基于区块链的会员隐私数据保护方法，数据写入时不需要会员进行验证，仅在 读取时需要用户验证，系统效率高。

具体实施方式

[0029] 为使本发明的目的、技术方案和优点更加清楚明白，下面结合实施例，对本发明作进一 步的详细说明，本发明的示意性实施方式及其说明仅用于解释本发明，并不作为对本发明的 限定。

[0030] 实施例1

[0031] 本发明基于区块链的会员隐私数据保护方法，包括以下步骤：

[0032] A、为每个会员匹配一个数据储存节点；

[0033] B、为每个数据存储节点匹配一个私钥，将私钥发送给对应的会员；

[0034] C、根据步骤B中匹配的所有私钥生成对应的公钥，将公钥在全网广播；

[0035] D、建立用户终端节点，为用户终端节点匹配一个密匙，将与密匙匹配的密钥发送给会 员系统的所有者；

[0036] 还包括数据写入的步骤：

[0037] E、会员系统的所有者通过秘钥进入用户终端节点；

[0038] F、用户终端节点提取需要写入信息的会员的公钥，将需要写入的信息通过公钥进行加密；

[0039] G、用户终端节点发起请求，请求为对应会员的数据存储节点创建一个新的数据区块，将加密后的需要写入的信息存储在新的数据区块中；

[0040] H、各节点通过共识机制校验达成步骤G中请求的合法性验证，通过校验后，新的数据 区块添加至对应会员的数据存储节点上；

[0041] 还包括数据读取的步骤：

[0042] J、会员系统的所有者通过秘钥进入用户终端节点；

[0043] K、用户终端节点发起请求，请求读取指定会员的数据；

[0044] L、各节点通过共识机制校验达成步骤K中请求的合法性验证，通过校验后，对应会员 的数据储存节点上连接的数据区块中的数据均发送到用户终端节点；

[0045] I、对应的会员使用手中的私钥对数据区块中的数据进行解密，获取对应的会员数据。

[0046] 采用上述方法，使用私钥对会员数据进行加密，私钥掌握在会员自己手中，需要查询会 员的数据存储节点上的会员数据时，需要使用会员手中的私钥对数据进行解密，因此，任何 人查看会员数据都需要经过用户的同意，而写入数据由于不涉及隐私问题，如果每次数据写 入都需要会员确认较为不便，因此本系统不需要用户确认也可写入数据。

[0047] 实施例2

[0048] 进一步的，所述步骤C中根据步骤B中匹配的所有私钥生成对应的公钥的方法采用RSA 公钥系统或椭圆曲线密码系统中的一种。

[0049] 所述步骤H中的共识机制为由用户终端节点完成校验。由于会员数据的写入有时涉及会 员系统所有者的权益，因此，写入时的共识机制为用户终端节点完成校验。

[0050] 所述步骤L中的共识机制为由指定会员的数据储存节点完成校验。由于会员数据的读取 涉及会员的权益，因此，读取时的共识机制为指定会员的数据储存节点完成校验。

[0051] 实施例3

[0052] 本实施例为实施例1的一种具体情况，基于区块链的会员隐私数据保护方法，包括一个 用户终端和5个用户，还包括以下步骤：

[0053] A、为每个会员匹配一个数据储存节点；

[0054] B、为每个数据存储节点匹配一个私钥，将私钥发送给对应的会员；

[0055] C、采用RSA公钥系统为所有私钥生成对应的公钥，将公钥在全网广播；

[0056] D、为用户终端建立用户终端节点，为用户终端节点匹配一个密匙，将与密匙匹配的密 钥发送给会员系统的所有者；

[0057] 还包括为会员A写入数据的步骤：

[0058] E、会员系统的所有者通过秘钥进入用户终端节点；

[0059] F、用户终端节点提取需要写入信息的会员A的公钥X，将需要写入的信息通过公钥X 进行加密；

[0060] G、用户终端节点发起请求，请求为对应会员A的数据存储节点创建一个新的数据区块，将加密后的需要写入的信息存储在新的数据区块中；

[0061] H、用户终端节点达成步骤G中请求的合法性验证，通过校验后，新的数据区块添加至 对应会员的数据存储节点上；校验失败后，用户终端节点发送错误报告到用户终端进行提示；

[0062] 还包括读取会员B数据的步骤：

[0063] J、会员系统的所有者通过秘钥进入用户终端节点；

[0064] K、用户终端节点发起请求，请求读取指定会员B的数据；

[0065] L、会员B的数据存储节点校验达成步骤K中请求的合法性验证，通过校验后，会员B的数据储存节点上连接的数据区块中的数据均发送到用户终端节点；校验失败后，用户终端 节点发送错误报告到用户终端进行提示；

[0066] I、会员B使用手中的私钥Y对数据区块中的数据进行解密，获取会员B的数据。

[0067] 以上所述的具体实施方式，对本发明的目的、技术方案和有益效果进行了进一步详细说 明，所应理解的是，以上所述仅为本发明的具体实施方式而已，并不用于限定本发明的保护 范围，凡在本发明的精神和原则之内，所做的任何修改、等同替换、改进等，均应包含在本 发明的保护范围之内。