软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2019,30(6):1661−1669 [doi: 10.13328/j.cnki.jos.005742]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

应用区块链的数据访问控制与共享模型*

王秀利, 江晓舟, 李 洋

(中央财经大学 信息学院,北京 100081)

通讯作者: 王秀利, E-mail: wangxiuli@cufe.edu.cn

摘 要: 数据已成为企业的重要资产.如何在企业内部对数据的访问权限进行有效控制、在企业之间安全共享数据一直是一个挑战.区块链中的分布式账本可以从某些方面解决上述问题,但是区块链所应用的非对称加密机制仅可进行一对一的安全传输,并不满足企业内部复杂的访问控制要求.提出一种应用区块链的数据访问控制与共享模型,利用属性基加密对企业数据进行访问控制与共享,达到细粒度访问控制和安全共享的目的.通过对比分析,该模型在安全性和性能上较好地解决了企业内部访问权限难控制、企业之间数据难共享的问题.

关键词: 区块链;平行区块链;属性基加密;访问控制;数据共享

中图法分类号: TP309

中文引用格式: 王秀利,江晓舟,李洋.应用区块链的数据访问控制与共享模型.软件学报,2019,30(6):1661−1669. http://www.jos.org.cn/1000-9825/5742.htm

英文引用格式: Wang XL, Jiang XZ, Li Y. Model for data access control and sharing based on blockchain. Ruan Jian Xue Bao/Journal of Software, 2019,30(6):1661−1669 (in Chinese). http://www.jos.org.cn/1000-9825/5742.htm

Model for Data Access Control and Sharing Based on Blockchain

WANG Xiu-Li, JIANG Xiao-Zhou, LI Yang

(School of Information, Central University of Finance and Economics, Beijing 100081, China)

Abstract: Data has become an important asset for an enterprise. How to effectively control access to data within an enterprise and securely share data between enterprises have been a challenge. Distributed ledger in blockchain can solve these problems in some ways. However, the asymmetric encryption mechanism applied by blockchain can only be transmitted peer to peer securely; it does not meet the complex access control requirements within the enterprise. This paper presents a model for data access control and sharing using block chain, and uses attribute based encryption to control and share enterprise data, so as to achieve the purpose of fine-grained access control and secure sharing. Through comparative analysis, the model can solve difficulties ofaccess control withinthe enterprise and sharing data between enterprises in security and performance.

Key words: blockchain; parallel blockchain; attribute-based encryption; access control; data sharing

对企业而言,数据越来越有价值,甚至已经上升到战略核心地位.企业关注的重点也从如何利用数据转向如何保护数据.传统的集中式存储存在许多安全隐患,若防火墙被攻克或数据泄露,将导致大范围数据丢失,而且也不利于企业内部多层级的访问控制需求和监督管理.区块链以数据难伪造、难篡改和可追溯引起了学术界和产业界的广泛关注[1],成为解决上述问题的关键技术.以比特币等数字货币为代表的区块链 1.0[2]解决了去中心

* 基金项目: 国家重点研发计划(2017YFB1400700); 国家自然科学基金(U1509214)

Foundation item: National Key R&D Program of China (2017YFB1400700); National Natural Science Foundation of China (U1509214)

本文由区块链与数字货币技术专题特约编辑斯雪明教授和陈文光教授推荐.

收稿时间: 2018-06-26; 修改时间: 2018-10-12; 采用时间:2018-12-18; jos 在线出版时间: 2019-03-27

CNKI 网络优先出版: 2019-03-27 16:40:31, http://kns.cnki.net/kcms/detail/11.2560.TP.20190327.1640.007.html

化等问题,但仍存在不足之处:(1) 交易完全透明且等待时间过长;(2) 在设计之初,有部分功能以规避监管为目的,并不适用于企业内部与行业内部;(3) 账户加密通常使用传统的非对称加密方式,在加密货币一对一的交易场景下可以提供很高的安全性,但对于企业内部场景,不便于灵活地访问控制,也不便于密钥的管理与保存.因此,传统区块链并不适合直接应用于企业.

对行业而言,同行业中的各个企业往往有合作与竞争的双重关系——既需要各个企业数据共享来完成整个行业版图的绘制,又需要保护好自己企业的数据.另外,各行业通常都有国家部门进行监管,如何在保证有效监管的同时又保护好各自的数据,成为了亟待解决的问题.

为解决上述问题,本文结合现实场景,分为企业内部与企业之间两部分,利用属性基加密(attribute-based encryption,简称 ABE)对区块链进行改进,提出一种新的企业内部访问控制与企业之间数据安全共享模型.

1 相关研究

1.1 区块链及相关技术

区块链是利用加密链式区块结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用智能合约来编程和操作数据的一种去中心化基础架构与分布式计算范式[3].比特币、莱特币是典型的公有链,所有节点中立、开放,并不适用于企业内部与行业内部.同时,由于所有节点都参与投票,交易的确认和区块的形成速度都非常慢.以比特币为例,每分钟确认 7 笔交易,每 10 分钟生成一个区块[4](为了确保安全,通常需要等待 6 个区块生成,即 1 小时完成交易确认),这在很多行业内是无法接受的.与公有链对应的是许可链,即只有被许可的节点才能参与投票、记账,其所有节点都在企业或行业内部,数量相对较少,因此响应速度较快.私有链、联盟链都属于许可链.

区块链通常使用单链结构,将账目、合约、交易等信息全部放在一条链上,所有参与计算的节点都在该链上投票以保证一致性.而这既没有保护隐私,又因大量冗余数据造成响应迟缓,平行区块链[5]应运而生.文献[6,7]提出了双链结构,所有参与的机构分享元数据及协议,但不分享数据.所有参与的机构都可以与其他机构交易,而保证隐私性.以此设计出两类区块链:(1) 仅存储账户信息和交易后的信息,但不执行交易的账户区块链;(2) 仅存储对交易有用的信息并且执行相关交易的交易区块链.这极大地提高了整个区块链的运行效率,同时,将账户自身变动与交易信息变动相分离,增加数据管理的灵活性.其所使用的双链结构主要用于金融领域,交易依然是一对一进行,未对原有非对称密码体制进行改动.

将区块链应用于数据共享,业内已有实践.如 Enigma[8,9]是一个分散的计算平台,拥有隐私性与可拓展性等特点.通过安全多方计算,其数据查询以分布式方式计算,任何一个节点都不能完整地访问数据.通过脱链存储技术,将区块链与分布式散列表[10]相关联,在区块链上仅保存数据存放的地址.MedRec 框架[11]将智能合约与访问控制相结合进行自动化的权限管理,实现了对不同组织的分布式医疗数据的整合和权限管理.

1.2 数据保护机制

非对称加密[12]是保证众多加密货币安全交易的基础之一,它包含 2 个密钥,即公钥和私钥.系统先以某种密钥生成算法(如 SHA256 Hash 算法[13]、Base58 转换),将输入经过计算得出私钥(一串固定长度的字符串),然后采用另一个算法(如 Secp256k1 椭圆曲线算法[14])分解私钥生成公钥,此过程是不可逆的.非对称加密在区块链中有两种用途:(1) 数据加密,用信息接收者的公钥对发送的信息进行加密,接收者以自己的私钥解密;(2) 数字签名,信息发送者以自己的密钥对信息哈希值加密(签名),接收者以发送者公钥解密后与原文哈希进行比对,用以确认此信息确实由发送者发送,达到不可伪造和不可抵赖目的.

区块链使用的椭圆曲线非对称加密机制虽然可以提供很高的安全性,但其密钥不可更改,且每个账户都要有单独的密钥.另外,加密货币只限于两个账户之间的交易,因此不存在权限管理问题.而在企业内部,这种加密方式难以满足大量员工对数据的多层级访问控制.

ABE[15−17]以属性为公钥,将密文、私钥与属性相关联,能更加灵活地表示访问控制策略.ABE 有以下优点:(1) 加密时只需要根据成员属性加密消息,而不需要关心群体中成员的数量和身份,降低了数据加密开销,也保

护了成员隐私;(2) 只有符合密文属性要求的群体成员才能解密消息,不符合属性要求的成员无法解密,从而保证了数据安全;(3) 用户密钥与随机多项式或随机数相关,不同用户的密钥无法联合,防止了用户的串谋攻击;(4) 支持基于属性的灵活访问控制策略,可以实现属性的与、或、非等门限操作.因此,ABE 在细粒度访问控制、隐私保护等方面具有良好的应用前景.

2 预备知识

2.1 访问控制树

使用树状图表示访问控制策略,以 T 表示.树中叶结点表示属性,非叶结点表示与、或等逻辑门限.设 $U=\{A_1, A_2,\ldots,A_n\}$ 是系统中的属性集合,$leaves(T)$ 表示 T 中所有叶结点集合.设 num_v 为 v 的子结点数,$k_v(1\leqslant k_v\leqslant num_v)$ 为 v 的门限值,以 $att(v)$ 表示与结点 v 有关的属性.给定一个属性集 U 和访问控制策略树 T_v,如下定义函数 $F(U,T_v)$.

- 若 v 是叶结点,当且仅当 $att(v)\in U$ 时,$F(U,T_v)=1$;
- 若 v 不是叶结点,设其子结点为 $v_1,v_2,...,v_{num_v}$,当且仅当存在至少 k_v 个子结点满足 $F(U,T_{v_i})=1$ 时($i\in\{1,2,\ldots,num_v\}$),$F(U,T_v)=1$;
- 在其他情况下,$F(U,T_v)=0$.

2.2 哈希算法

哈希算法是一个函数,将任意长度的数据作为输入,都将被映射为固定长度的字符串.同时,它也是一个单向函数,由输入可以轻易地算出数据的哈希值,却无法由哈希值逆向推出原数据.

Merkle 树[18]是基于哈希算法的树型数据结构,每个非叶结点都是其叶结点的哈希值.将数据进行分组哈希,并将生成的新哈希值插入到树中,如此递归,直到只剩最后一个根哈希值.相较于对所有数据打包进行哈希计算而言,这极大减少了工作量.以图 1 为例,当加密文件 3 出现改动时,需要更新哈希值,若不使用 Merkle 树,则要把所有 4 个文件重新哈希;而使用 Merkle 树,则只需重新计算哈希值 3 和 6,便可以得到新的根哈希值.

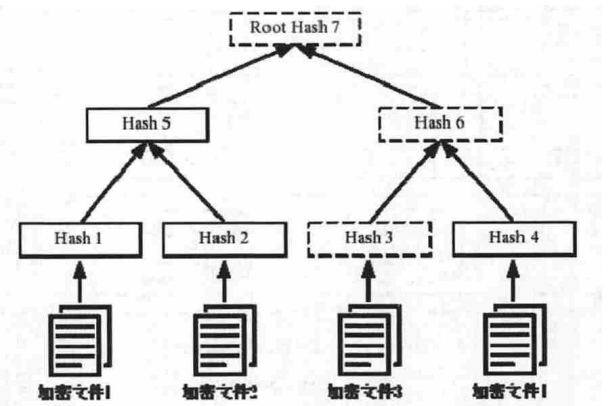

Fig.1 Merkle tree

图 1 默克尔树

3 访问控制与共享模型及方案

3.1 模 型

本模型分为 5 层:存储层、区块链服务层、API 层、链上代码(智能合约)层、应用层,其架构如图 2 所示.

- 存储层:为快速生成检索区块,采用链下存储方式,即链上只存储数据地址,原数据经过对称加密后存储在底层数据库,由企业维护.存储层设在企业内部,其存储结构可以使数据拥有者在将数据存入时决定数据的访问控制策略;
- 区块链服务层:分为企业链(company blockchain,简称 CBC)和行业链(industry blockchain,简称 IBC).其

中,CBC 记录企业内部的数据存储地址与变化情况,由企业内部节点共同维护,确保不同节点状态一致,提供基于属性的访问控制服务;IBC 记录行业内部企业之间的数据交换与调用,数据的请求与共享都将记录在 IBC 上以便查询和监管;

- API 层:接口用于数据的查询、区块广播、发送等;
- 链上代码层:提供智能合约服务.主要功能是提供属性基访问控制,即在 CBC 与 IBC 上提供自定义的访问控制策略,只有满足特定属性(或级别)的账户才能读取(或写入)数据;
- 应用层:提供各种应用程序,如监管系统、查询系统等.

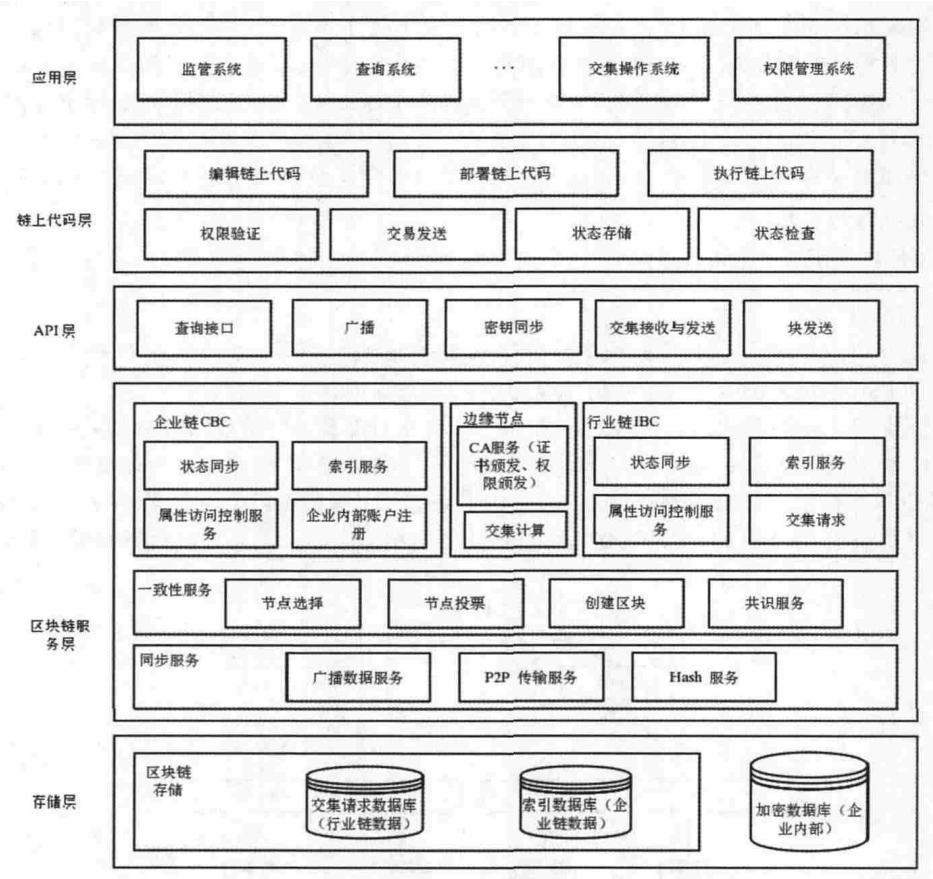

Fig.2 Model architecture

图 2 模型架构

无论企业内部还是行业内部,都是弱信用环境.因此本模型基于联盟链,即只有被许可的节点才能进行读写操作.同时摒弃了公有链常用的 POW,POS 等共识机制,而是使用信用制,当发现节点有违规写入垃圾信息或其他作恶行为,则直接将其剔除出整个系统,收回其权限.

整个行业区块链系统由 3 种节点维护,分别为企业节点、行业节点与边缘节点,节点之间关系如图 3 所示.各自职能如下.

(1) 企业节点:用于维护企业链.当新数据达到阈值后,企业节点将数据经过对称加密后存放至底层数据库,并将其存放地址和密钥及 Merkle 树一同放到链上用于查询与验证;

(2) 行业节点:用于维护行业链而非企业内部数据,由行业协会或行业内所有企业共同维护,用于确认行业内各企业之间的数据交互(数据交集查询).行业节点仅维护行业链而不属于任何企业链.其主要功能是便于监管机构或行业协会对行业链进行监管;

(3) 边缘节点:同时加入企业内部区块链网络与行业区块链网络,用于连接企业链与行业链,进行数据传递.企业链与行业链使用同一套属性基加密算法,将授权中心 CA 部署在边缘节点可以提高资源利用率.当某企业在行业链上发出数据共享请求时,其他企业边缘节点上的智能合约自动验证其访问权限,并进行交集操作.

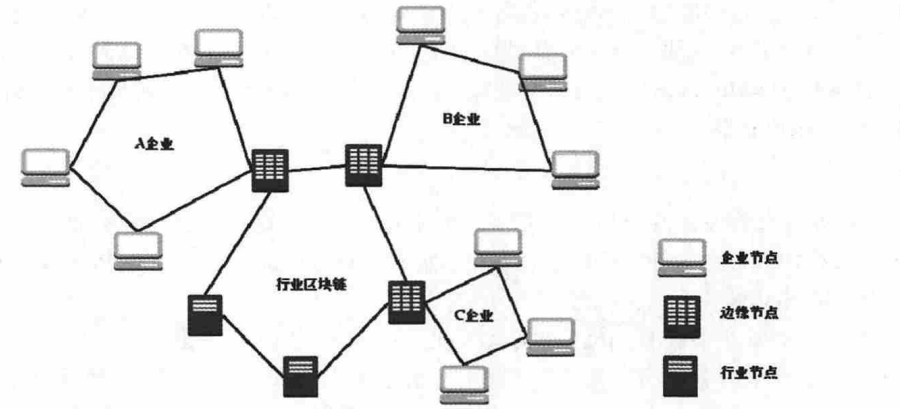

Fig.3 Peers diagram

图 3 节点关系示意图

整个系统包括企业链与行业链两部分,是平行区块链结构:企业链负责存储具体数据的位置索引,行业链负责记录企业之间的数据交集操作.具体如下.

(1) 企业区块链:确保企业内部数据的安全与可追溯.

当缓存区中的数据达到阈值,企业内部节点将其加密后传输至底层数据库中,同时将数据的输入时间戳、区块长度及前一个区块的哈希值作为区块头,根据访问控制树将数据位置索引、明文形式的访问控制策略和数据 Merkle 根加密后打包成块,存储至区块体中,其后上传至企业链上.其数据存储结构如图 4 所示.

(2) 行业区块链:将行业内各企业置于监管之下,并可通过多方计算将所有企业的数据进行统一分析.

与企业链中的准备工作相同,每个企业在将数据位置索引上传至企业链时,将行业内其他企业的属性也纳入访问控制树中,一个典型的属性基加密策略树如图 5 所示.其左支代表对企业的属性要求,右支代表企业中有权限部门的账户要求.只有特定企业中的特定部门才能进行解密.数据请求者在提出数据交集请求时,需将所请求数据与含有自己属性的令牌一同发布至行业区块链上.所有企业的边缘节点都将验证其是否有访问本企业数据的权限,只有通过权限验证,边缘节点才会自动对所请求的数据进行交集操作,并返回给请求企业.由于属性基访问控制策略的存在,全行业链节点都将记录这一过程,但只有交易双方可见交易的细节.另外,对于需要监管者查看所有数据的行业,可直接将监管者属性列入访问控制树左支,即可使其拥有访问权限.

Fig.4 Blockchain storage structure

图 4 区块体存储结构

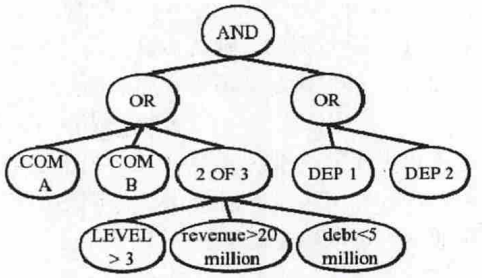

Fig.5 Attribute based encryption strategy tree

图 5 属性基加密策略树

数据存储方面,本模型使用了密文存储与脱链存储来保证数据的安全.

(1) 密文存储:由于系统主要功能是保护企业内部重要数据,通常是用户隐私数据、财务数据等,因此底层存储应采用密文存储.而直接使用非对称加密会导致密钥管理混乱,同时对于大量底层数据而言效率不高.因此,选用对称加密方式对底层数据进行加密;

(2) 脱链存储:由于区块链处理速度较慢,不适宜将所有数据直接存储在链上,因此使用脱链存储.通过建立分布式散列表,区块链存储对数据的引用,而非数据本身.数据在存储时进行加密,并编辑数据访问控制策略.Merkle 树保证了数据即使没有存在链上,也不能被篡改,且在部分数据变动后可以较小代价更新 Merkle 根.

3.2 方 案

该方案由企业链与行业链两个相互隔离又可通过边缘节点相互通信的双链系统组成,其中:企业链用于加密存储企业内部数据的地址,行业链则用于记录行业内部企业之间的数据请求.具体步骤如下.

3.2.1 企业内部访问控制

(1) 初始化:根据安全参数 1^{λ},由授权中心 CA 执行产生主私钥 mk 和公共参数 pp;

(2) 身份注册:企业内各部门向系统提出注册申请,获取其真实身份信息对应的标识 UID 及属性集合 S_U;

(3) 密钥分发:按照密钥分发算法 $KeyGen(mk,S_U)$,CA 根据注册者属性集 $U \in S_U$,计算其属性私钥、属性参数,并由此计算出使用者的私钥 SK,将其通过安全信道发送给使用者保存;

(4) 加密数据:数据上传者根据访问者的属性对数据制定访问控制策略树 $StrGen(S_U) \rightarrow T_{com}$,随机生成对称加密密钥 rs,数据经过对称加密计算后放入底层数据库.对称加密算法可以表示为

$$SEnc_{rs}(D(d_1,d_2,d_3,\ldots,d_n)) \rightarrow cph;$$

(5) 数据上传:企业节点根据访问控制策略树对数据索引地址 add、对称加密密钥 rs 进行加密,并将其广播至区块链.同时,节点生成该数据索引 id 与链上数据的映射,将其放入底层数据库(不与经对称加密后的数据一同存放):

$$\begin{aligned} &AddGen(cph) \rightarrow add \\ &AEnc_{T_{com}}(add,rs) \rightarrow CPH \end{aligned};$$

(6) 访问密文:访问者根据数据索引 id 在链上查得该数据的地址与对称加密密钥.若该访问者没有权限访问此数据,则无法得到密钥 rs,无法对索引地址进行解密,也就无法访问原数据;若该访问者属性满足访问控制策略树,则其可以解密得到地址 add 与密钥 rs,可以至底层数据库访问该数据:

$$\begin{aligned} &Dec(CPH) \rightarrow add,rs \\ &SDec(cph,rs) \rightarrow D(d_1,d_2,d_3,...,d_n) \end{aligned}.$$

3.2.2 行业内部访问控制

(1) 前 4 步与企业内部数据访问控制相同,但在对数据加密时,其访问控制策略树不仅考虑企业内部账户,还加入行业内其他可进行交集操作的企业属性 $S_{U'}$,$StrGen(S_{U'}) \rightarrow T_{ind}$;

(2) 令牌生成:每个企业生成一个 token 令牌,包含该企业的权限与属性信息;

(3) 加密请求:请求数据的企业将需要与其他企业进行交集操作的数据 $D(d_1,d_2,d_3,\ldots,d_n)$用访问控制树 T_{ind} 进行加密,使其仅满足被请求企业的属性:

$$Enc_{T_{ind}}(D(d_1,d_2,d_3,...,d_n)) \rightarrow cph;$$

(4) 发送交集操作请求:请求数据企业将加密后的数据与自己的令牌一同发送至行业区块链上,所有企业都可以看到并记录这一消息,并由令牌中的信息判定其来源,但只有符合密文中所包含的访问控制树的企业节点可以解密此消息:

$$Dec(cph,token) \rightarrow D(d_1,d_2,d_3,\ldots,d_n);$$

(5) 交集操作:由于边缘节点既是企业链的节点,又是行业链的节点,被请求方的边缘节点在完成解密后,可以自动在其内部企业链上检索该数据是否开放给请求方.若接收到的令牌可以满足交集数据的访

问控制树,则边缘节点自动将数据进行交集操作,并通过安全信道返回给请求方:

$$SI(D_A,D_B)\rightarrow D_{A\cap B};$$

(6) 上传区块链确认:当请求方完成交集操作后,全局广播一条包含此令牌的数据,表明已完成交集操作,其他企业确认后将此行为记录在行业区块链上.

以 *A*,*B*,*C* 这 3 家处于同一个行业链中的企业为例.*A* 为数据请求方,*B* 和 *C* 为数据共享方.其中,*B* 在企业链的访问控制树中将本年度 1 月~3 月数据设为对 *A* 可操作,而 *C* 只共享了一月数据给 *A*.*A* 试图请求 *B*,*C* 的 1 月、2 月数据用作交集操作,则将自己 1 月、2 月数据经过 $Enc(D(Jan_A,Feb_A))$得到 cph_A,此密文所含访问控制树仅 *B*,*C* 可解密.将 cph_A 连同 $token_A$ 发送至区块链.*B* 和 *C* 都将接收到此信息,但边缘节点用 $token_A$ 尝试解密各自的 1 月、2 月数据时,只有 *B* 能完成操作,则 *B* 的边缘节点将 $D(Jan_B,Feb_B)\cap D(Jan_A,Feb_A)$返回给 *A*,*C* 返回空.在 *B*,*C* 都完成上述操作后,*A* 将自动向区块链广播一条消息表明已完成交集操作.

假设 *B* 在企业链的访问控制树中将数据 d_1,d_2,d_3 设为对 *A* 可操作,而 *C* 只共享 d_1 给 *A*.*A* 向 *B* 和 *C* 提出 d_1,d_2,d_3 数据交集申请的具体算法如下.

算法.

1. *B*,*C* 利用 $StrGen(S_U)$分别生成各自的 T_{indB} 和 T_{indC};

2. *B*,*C* 分别使用随机生成的对称密码对数据加密:

$$SEnc_{rs_B}(D_B(d_1,d_2,d_3))\rightarrow cph_B SEnc_{rs_C}(D_C(d_1))\rightarrow cph_C;$$

3. *B*,*C* 根据各自策略树对数据地址索引与对称密码加密:

$$\begin{aligned}&AddGen(cph_B)\rightarrow add_B\\&AddGen(cph_C)\rightarrow add_C\\&AEnc_{T_{com_B}}(add_B,rs_B)\rightarrow CPH_B\\&AEnc_{T_{com_C}}(add_C,rs_C)\rightarrow CPH_C\end{aligned};$$

4. 数据上链:

$$\begin{aligned}&CPH_B\rightarrow CBC_B\\&CPH_C\rightarrow CBC_C\end{aligned};$$

5. *A* 向 *B*,*C* 发起交集请求,*B* 的边缘节点将会进行如下操作:

$$\begin{aligned}&Dec(cph_B,token_A)\rightarrow D_B(d_1,d_2,d_3)\\&SI(D_B(d_1,d_2,d_3),D_A(d_1,d_2,d_3))\rightarrow D_{A\cap B}\end{aligned};$$

对于 *C*,由于 *A* 不满足 *C* 设定的交集访问权限,因此无法使用 Dec 算法解密数据,返回 *null*.

6. *A* 在完成上述操作后,将此操作上传至行业区块链 IBC,使行业链上的其他企业都记录下这一操作过程:

$$REQ((A\rightarrow B,C),D(d_1,d_2,d_3))\rightarrow IBC.$$

4 对比分析

表 1 从数据安全、企业间弱信用环境和数据存储等方面将本模型与传统区块链进行对比分析.

5 结束语

随着区块链的快速发展,越来越多的应用场景被开发出来,其在数据存储与共享方面的研究与实践也受到广泛关注.本文提出一种应用区块链的数据访问控制与共享模型,用属性基加密对现有区块链的加密方式、数据存储方式进行了改进,以满足数据在企业内部的访问控制以及企业之间数据共享的需求,达到了细粒度访问控制与安全共享的目的.其中,脱链存储、非对称加密与对称加密相结合的措施已可在 Hyperledger Fabric[19]等平台上实现.

Table 1 Comparative analysis between the model and traditional blockchain

表 1 本模型与传统区块链对比分析

		本模型及其优势	传统区块链
数据安全	企业内部访问控制	对于企业内部复杂的等级和权限,采用 ABE 进行细粒度访问控制	只能进行一对一传输,无法满足需求
	黑客攻击与数据泄露	所有底层数据都经过加密,受到攻击或数据泄露时仍可保证信息安全	链上数据透明,进入系统可看到所有数据
企业间弱信用环境	信用	不同企业间既有合作也有竞争,本模型可使其在弱信用环境下共享数据	更适用于完全无信用关系的场景
数据存储	数据滥用	企业每次发出请求都被记录在链上,并被其他企业观测到,因此随意进行数据请求不可行	缺少有效的访问控制策略,无法阻止恶意节点或需要大量算力维护以保持节点不作恶
	存储空间利用率	企业链上记录了每个文件的访问控制策略,行业链上只需记录和确认交集操作请求即可	所有数据都记录在链上

References:

[1] 2018 China blockchain industry white paper. MIIT, 2018 (in Chinese). http://www.miit.gov.cn/n1146290/n1146402/n1146445/c6180238/part/6180297.pdf

[2] Swan M. Blockchain: Blueprint for a New Economy. O'Reilly Media Inc., 2015.

[3] Yuan Y, Wang FY. Blockchain: The state of the art and future trends. Acta Automatica Sinica, 2016,42(4):481−494 (in Chinese with English abstract). [doi: 10.16383/j.aas.2016.c160158]

[4] Bitcoin traffic bulletin (redux). http://hashingit.com/analysis/44-bitcoin-traffic-bulletin-redux

[5] Yuan Y, Wang FY. Parallel blockchain: Concept, methods and issues. Acta Automatica Sinica, 2017,43(10):1703−1712 (in Chinese with English abstract). [doi: 10.16383/j.aas.2017.c170543]

[6] Tsai WT, Yu L, Wang R, Liu N, Deng EY. Blockchain application development techniques. Ruan Jian Xue Bao/Journal of Software, 2017,28(6):1474−1487 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5232.htm [doi: 10.13328/j.cnki.jos.005232]

[7] Tsai WT, Blower R, Zhu Y, Yu L. A system view of financial blockchains. In: Proc. of the IEEE Symp. of Service-oriented System Engineering. IEEE, 2016. 450−457. [doi: 10.1109/SOSE.2016.66]

[8] Zyskind G, Nathan O, Pentland A. Decentralizing privacy: Using blockchain to protect personal data. In: Proc. of the IEEE Security and Privacy Workshops. IEEE, 2015. 180−184. [doi: 10.1109/SPW.2015.27]

[9] Zyskind G, Nathan O, Pentland A. Enigma: Decentralized computation platform with guaranteed privacy. 2015. https://enigma.co/enigma_full.pdf

[10] Maymounkov P. A peer-to-peer information system based on the XOR metric. In: Proc. of the IPTPS. LNCS 2429, Springer-Verlag, 2002. 53−65. [doi: 10.1007/3-540-45748-8_5]

[11] Ekblaw A, Azaria A, Halamka JD, MD, Lippman A. A case study for blockchain in healthcare: "MedRec" prototype for electronic health records and medical research data. Technical Report, 5-56-ONC, Massachusetts Institute of Technology, 2016. https://www.healthit.gov/sites/default/files/5-56-onc_blockchainchallenge_mitwhitepaper.pdf

[12] Stinson DR, Paterson M. Cryptography: Theory and Practice. 4th ed., CRC Press, 2018.

[13] FIPS 180-2. Secure Hash standard. http://csrc.nist.gov/publications

[14] SEC 2: Recommended elliptic curve domain parameters. 2010. http://www.secg.org/sec2-v2.pdf

[15] Sahai A, Waters B. Fuzzy identity-based encryption. In: Proc. of the EUROCRYPT. LNCS 3494, Springer-Verlag, 2005. 457−473. [doi: 10.1007/11426639_27]

[16] Goyal V, Pandey O, Sahai A, *et al*. Attribute-based encryption for fine-grained access control of encrypted data. In: Proc. of the ACM Conf. on Computer and Communications Security. ACM Press, 2006. 89−98. [doi: 10.1145/1180405.1180418]

[17] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption. In: Proc. of the IEEE Symp. on Security and Privacy. IEEE, 2007. 321−334. [doi: 10.1109/SP.2007.11]

[18] Merkle RC. A digital signature based on a conventional encryption function. In: Proc. of the CRYPTO. LNCS 293, Springer-Verlag, 1987. 369−378. [doi: 10.1007/3-540-48184-2_32]

[19] Hyperledger whitepaper-wg. https://wiki.hyperledger.org/groups/whitepaper/whitepaper-wg

附中文参考文献:

[1] 2018 年中国区块链产业白皮书.工信部,2018. http://www.miit.gov.cn/n1146290/n1146402/n1146445/c6180238/part/6180297.pdf

[3] 袁勇,王飞跃.区块链技术发展现状与展望.自动化学报,2016,42(4):481−494. [doi: 10.16383/j.aas.2016.c160158]

[5] 袁勇,王飞跃.平行区块链:概念、方法与内涵解析.自动化学报,2017,43(10):1703−1712. [doi: 10.16383/j.aas.2017.c170543]

[6] 蔡维德,郁莲,王荣,刘娜,邓恩艳.基于区块链的应用系统开发方法研究.软件学报,2017,28(6):1474−1487. http://www.jos.org.cn/1000-9825/5232.htm [doi: 10.13328/j.cnki.jos.005232]

王秀利(1977－),男,山东高唐人,博士,副教授,CCF 高级会员,主要研究领域为金融科技,人工智能与安全.

江晓舟(1995－),男,硕士生,主要研究领域为区块链.

李洋(1981－),男,博士,副教授,CCF 专业会员,主要研究领域为信息安全.