一种基于区块链上的数据安全共享加密方案

徐雪松[1、2]，金泳[1]，曾智[1]

[1]（新零售虚拟现实技术湖南省重点实验室，湖南商学院，长沙 410205）

[2]（智能物联网信息安全湖南省工程研究中心，湖南，长沙 410205）

通讯作者：金泳, E-mail: 172185172@qq.com

摘要：区块链因其防篡改、可追溯和去中心化的特点，在数据安全方面具有广阔的应用前景。但是现有加密方法无法保障用户数据的隐私，需要一种新的方案使用户数据在安全共享和隐私保护之间达到一种完美的平衡。因此，本文提出一种基于同态加密的区块链数据安全共享方案，该方案由一个可信的第三方生成一对同态密钥作为全网的同态密钥，对用户数据经同态加密后提交全网验证，然后接受方利用同态私钥解密，获得共享的数据。同态加密技术可以实现无密钥方对密文的计算，密文计算无须经过密钥方，既可以减少通信代价，又可以转移计算任务，保护用户数据隐私。

关键词：区块链；数据安全；同态加密；安全共享

A Secure Data Encryption Scheme Based on Blockchain

XU xue song[1、2] JIN yong[1] ZENG zhi[1]

[1](Key Laboratory of Hunan Province for New Retail Virtual Reality Technology, Hunan University of Commerce, Changsha 410205, China)

[2]（Engineering Research Center of Hunan Province for Intelligent Internet of things information security technology , Hunan Changsha 410205,China）

Abstract: Due to its characteristics of tamper resistance, traceability and decentralization, blockchain has broad application prospects in data security. However, existing encryption methods cannot guarantee the privacy of user data, and a new solution is needed to achieve a perfect balance between user data and secure sharing and privacy protection. Therefore, this paper proposes a blockchain private data security sharing scheme based on homomorphic encryption. This scheme generates a pair of homomorphic keys as a homomorphic key of the whole network by a trusted third party, and the user data is the same. After the state is encrypted, the whole network is submitted for verification, and then the recipient uses the homomorphic private key to decrypt and obtain the shared data. The homomorphic encryption technology can realize the calculation of ciphertext by the keyless party. The ciphertext calculation does not need to go through the key side, which can reduce the communication cost, and can transfer the computing task and protect the user data privacy.

Key words: Blockchain; data security; homomorphic encryption; secure sharing

---

基金项目:国家自然科学基金重大项目（国家安全管理的决策体系设计 项目编号：71790615）;湖南省社科成果评审委员会项目（项目编号：XSP18YBZ123）

Foundation item: National Natural Science Foundation of China (National Safety Management Decision System Design Project No.: 71790615) ; Hunan Provincial Social Science Achievements Review Committee Project (Project No.: XSP18YBZ123)

采用数据共享机制来挖取数据背后的潜在价值，随着数据价值的攀升以及数据规模的壮大变的越来越重要。让数据信息拥有者与数据需求者相互之间彼此信任、避免非法获取数据或者攻击是数据共享的基本共识。中心化的共享方案是传统的数据共享所能依靠的最经典的方案，虽然能够解决共享中互不信任、数据无法共享的问题，但缺点是数据都集中存储在第三方机构中，一旦第三方机构受到攻击，数据在共享时仍无法避免被删除或更改的风险。区块链技术采用的是非对称加密的算法，哈希算法和数字签名算法等使其具有去中心化的特点，能够有效解决恶意攻击以及改变目前传统的中心化机制的问题。原因是采用非对称的加密算法，使得数据的删除或更改变得几乎不可能，以此增加了数据在共享时的可信度和安全性。区块链可以看作是全网公开透明的一个账本，由于交易都是透明的，因此会存在隐私数据的泄露。例如政府的一些数据属于私密的，但在特殊的情况下需要共享。因此为了保证能够更加安全的共享一些隐私数据，而减少在共享时数据泄露的现象，就需要将数据加密存储在区块链中。在打破数据孤岛的现象下，机密数据的泄露现象依旧会存在，此时，传统的哈希函数加密方法已不足以支撑隐私数据的安全共享，以此需要一种新的加密算法，确保隐私数据既能安全加密共享，又能降低泄露隐私数据的程度。同态加密是一种能够在原有基础上使用区块链技术、无需提前解密加密数据就可以执行计算的方法。通过使用同态加密技术，在区块链上存储数据、共享数据时不会改变区块链的属性，可以达到一种完美的平衡，也不会造成任何重大的变动。由于区块链上的数据会被加密存储然后进行安全共享，但考虑到区块链存储数据的隐私问题，使用同态加密技术能够使公有区块链具有私有区块链的数据隐私保护效果。同态加密技术不仅提供了隐私保护，它同样允许随时访问公用区块链上的加密数据进行审计或其他目的。使用同态加密在公用区块链上存储数据将能够同时提供公有和私有区块链的最好的部分。因此本文采用同态加密技术，提出一种基于区块链上的隐私数据安全共享的方案，以期为数据安全共享提供一定的借鉴。

国内外学者针对科学数据共享领域中参与主体行为、共享动力与障碍、共享影响因素等展开了持续性的研究。孙晓燕通过理论模型验证了社会科学家的共享行为被感知职业获益和风险、感知努力和数据共享态度影响[1]。庄倩等通过建立演化博弈模型，分析了科学数据共享的动态演化过程[2]。陈欣等从个体驱动、科研驱动、社会驱动层面，借助了扎根理论，构建了社会科学数据共享驱动因素核心范畴[3]。何琳等引入TPB 和 TAM 构建科学数据共享意愿模型，对影响因素进行了验证[4]。张晋朝认为科研人员的自我价值感知、互惠预期、人际信任等是形成数据共享信念的重要维度[5]。S.B.Linek 等研究科研人员个性对数据共享社会困境的影响，探讨其与共享态度、共享动力与障碍、共享意愿、实际共享行为的关联度[6]。K.Williamson 等深入探讨公民科学家数据共享障碍以及专业科学家接受公民科学家数据共享的障碍[7]。对于基于区块链的其他数据共享方面，董祥千等借助区块链技术建立了一种全新的去中心化数据共享模型，模型中采用的是安全多方计算及差分隐私技术保障数据所有者的计算和输出隐私[8]。在信息物理融合系统下，丁庆洋等提出了融合区块链技术与 CPS 的防护思想，构建了实现二者深入融合的 BCCPS 框架机制，使得在此系统上的信息能够安全共享[9]。医疗数据安全共享困难一直都是医疗行业的一大痛点，薛腾飞等提出了一个基于区块链的医疗数据共享模型，适用于解决各医疗机构数据安全共享的难题[10]。由此不难看出，由于共享经济独特的发展特征，数据之间的安全共享已经变得越来越重要。近年，我国学者在同态密码学研究上发表了一些成果，在探索过程中，将同态加密技术应用多在云计算、多方计算、匿名访问、电子商务等领域[11]。但也有一些学者结合了区块链与同态加密的特征，设计发明了一些专利，例如梁秀波等人发明了基于加法同态加密的区块链的隐私保护方法[12]、郑珂威也设计发明了基于完全同态加密的区块链信息加密方法，以及华为公司也利用了同态加密的算法以实现区块链的安全隐私保护。

1 相关知识

1.1 区块链相关技术

目前，关于区块链的研究越来越多，但却尚未形成一个公认的区块链定义，最为广泛的定义是区块链是一种以块链结构存储数据，并由多方共同维护，使用密码学技术保证传输和访问安全，能够实现数据永久存储、无法篡改、无法侵入的技术体。换言之，区块链就是利用计算机程序在全网记录所有交易信息的

一个分布式中心化账本[13]。区块链分为狭义区块链和广义区块链，狭义区块链主要是以区块链技术应用，只是一个分布式账本，是业内一种“弱区块链”的观点。广义的区块链其实才是核心，就是把区块链思维应用到各个领域产业中。从狭义来讲，区块链是一种数据结构。是按照时间顺序，将有效的数据块以链条的形式链接而成的，并以密码学的方式保证数据的不可篡改性和不可抵赖性。从广义来说，区块链技术则是一种去中心化的分布式计算范式[10]。以加密链式来验证与存储数据、以分布式共识算法来生成和更新数据，以及智能合约（自动化脚本）来编程和操作数据。

区块链的安全机制实则是依据它的原理决定的，区块链采用的是分布式存储，利用点对点的组成方式联结网络。每一个节点都可以保存区块链全部数据的信息，如此是为了避免由传统的中心节点存储时，一旦中心节点受到攻击而全部的数据信息受到损失的情况。点对点的分布式存储可以建立节点之间的信任关系，也可以避免对于单一节点的过量访问导致网络拥挤的现象。

区块链技术是利用密码学算法将数据信息存储在相应的区块中，例如哈希算法。哈希算法是通信领域中一种重要的技术，是将大小不一的数据通过数学算法映射成固定大小的字符串。加密的哈希算法是一个散列函数，虽然可以很容易的算出数据的哈希值，但反过来根据已知的哈希值却很难算出原始的数据。更重要的是一旦区块中的任意数据发生更改，该区块头中的哈希值也会相应发生改变。区块链中区块是以链的形式头尾相连，因此一个区块的哈希值发生改变，后续的区块都会发生变化。区块链中的共识机制，使得全部节点都保存了该区块的原始值，若非要强行更改数据，则需要花费全网 51%的算力使攻击不轻易成功。

1.2 同态加密基本知识

同态加密概念的首次提出是 Rivest 等学者 1978 年的题为《On databanks and privacy homomorphic》[14]中，允许用户直接对密文进行特定的代数运算后得到的数据仍是加密的结果，等同于对明文进行同样的操作，结果加密一样。与一般的加密算法相比，同态加密不仅能够实现最基本的加密操作还能够实现密文中的多种计算功能。采用同态加密技术可以不需要花费高昂的计算代价计算解密每一个密文，而是先计算多个密文后再进行解密。同态加密的主要特点是密文计算不需要经过密钥方，以此减少通信的代价以及转移计算任务，以用来提高数据安全存储共享的安全性。数据的共享之间采用同态加密技术，可以实现让解密方获知最后的结果，无法得知每一条密文的消息，从而减少数据共享过程中，私密数据的泄露。

同态加密不仅包含乘法的同态加密，也包含了加法的同态加密。同态加密一般是由四个部分组成：密钥的生成、同态加密、同态解密以及同态赋值。密钥的生成是由安全参数 λ 生成公钥 pk、私钥 sk。同态加密是指给出指定明文 m∈{0，1}*，用公钥 pk 将其加密，得到密文 c。同态解密是指输入私钥 sk 和密文 c 进行解密计算，输出明文 m'。同态赋值是指输入公钥 pk，t 个输入的电路 C，一组密文 $c=(c_1,c_2,\cdots,c_t)$，输出 c*=evaluate(pk，C，c)，且满足 dec(sk，c*)= C（$m_1,m_2,\cdots,m_n$）。其中 evaluate 算法是完全同态加密中最重要的部分，通过 evaluate 算法可以对任意函数进行计算，输入都是密文，可以计算解密函数。

2 数据加密共享的机制

区块链技术的本身使得数据对每个参与方都是可达的，即用户的数据对各个参与方是透明的，任何组织都可以访问到相同的数据。如果将用户的隐私数据放到链上将会放大用户隐私泄露的风险，例如在比特币等公有链系统中，所有的交易信息都是公开的，包括交易金额。然而，在公共管理部门如政府数据的交易中，数据交易信息包含了部分政府内部敏感数据，非政府内部相关方不能查看，且同时要满足如今阳光下执法的监管要求，部分政府数据需要共享公开。目前，大部分的区块链并没有满足数据的隐私性要求，针对该问题本文提出了提一种隐私数据安全共享加密机制，保障了需求数据在共享过程中不泄露隐私数据。

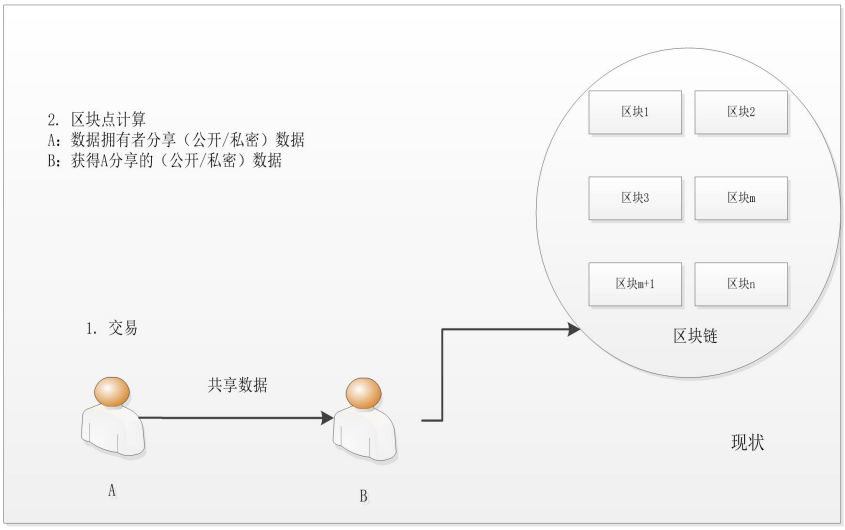

Fig.1　Schematic diagram of the status of blockchain shared data

图 1　区块链共享数据现状示意图

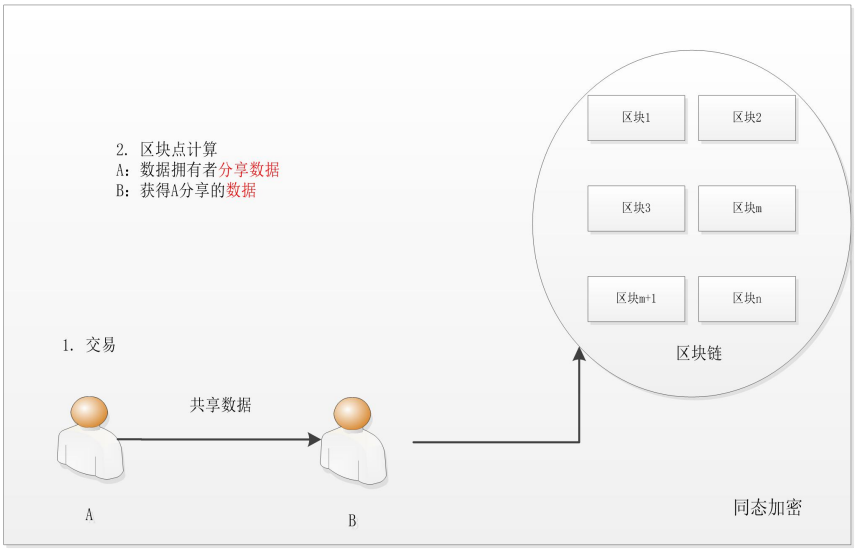

Fig.2　Schematic diagram of data sharing in a homomorphic encrypted blockchain

图 2　同态加密区块链共享数据示意图

如上图中 A 向 B 共享 B 所需的数据，需要区块链节点共识，但是 A 不想让区块链节点知道共享的数据类型（公开数据/隐私数据）。同态加密技术通过不需要经过密钥放而进行密文计算，既可以实现无密钥方对密文的计算，又可以减少通信代价和转移其计算任务，平衡各方的计算代价。数据共享可以看成是两个地址之间的交易，是一种进行可靠、具有公信力的数据传递。对于数据的安全共享，可以提供一个同态加密库，对用户的交易数据用其公钥进行加密保护，交易的时候都是密文运算，最终区块链中加密保存。即使节点被攻破，获取到区块记录也无法解密；其次再进行范围证明校验，背书节点能够对密文进行背书，无需解密就能校验交易的正确性，如校验交易数据是否是需求方需要的，从而识别出恶意交易风险，保证了智能合约的正确执行。

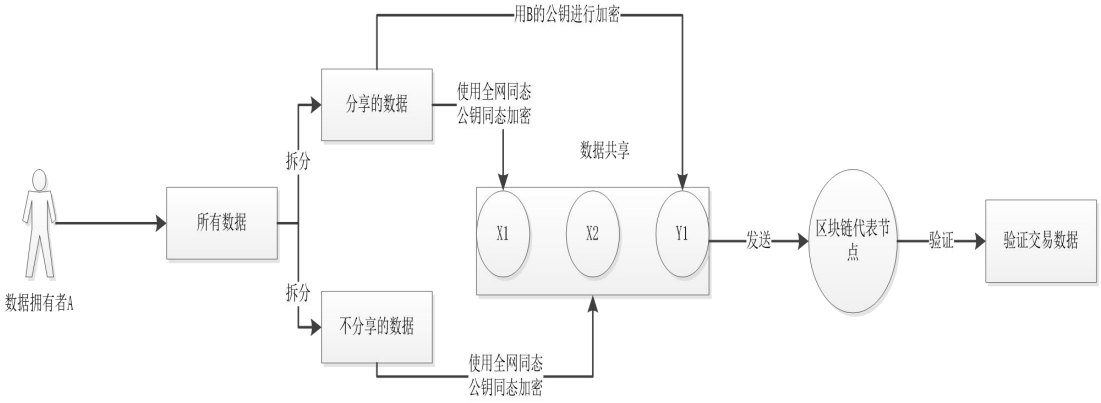

Fig.3 data encryption sharing mechanism

图 3 数据加密共享机制

本文提出了的一种基于区块链上的数据安全共享机制，步骤如下：

(1)同态密钥的生成，由一个可信的第三方生成一对同态密钥作为全网的同态密钥；公开公钥，私钥保存在第三方中，可用于用户在丢失了自己的数据申请情况下，通过本人的申请操作重新可见数据分享情况；

(2)拆分数据拥有者的数据，需要分享的数据以及不分享的隐私数据；

(3)使用全网公开的公钥加密拆分后分享的数据以及不分享的数据，此加密采用加法同态加密算法；

(4)使用数据接收方的公钥加密需要分享的数据，此加密算法采用加法同态加密算法；

(5)数据拥有者发起数据共享的交易，将加密后的密文发送至区块链，区块链选取一个代表节点进行验证交易数据。

模拟一个数据拥有者分享所需数据给数据接收者 B 的交易，如图 3 所示。首先，A 在自己的数据存储方将自己的数据拆分为需要分享的数据，以及不需要分享的数据，然后用全网同态公钥加密拆分后的两种数据，密文记为 X1、X2，并用 B 的公钥再次加密需要分享的数据得密文 Y1，A 发起交易，交易的信息包括 X1、X2 和 Y1，将交易发布到区块链上，然后选取一个代表节点对此次的交易进行验证，并将这次的交易记录上链到全网，此为一个完整的数据共享交易过程。

3 变体同态加密方案[16]

在基于文献[15]的研究上，文献[16]提出了一种新的同态加密算法，经过评判方案的性能、安全性、以及同态性都与文献[15]的加密功能区别不大。虽然新的加密方案的算法计算复杂性相比前一算法是难度较大，但经过两个方案的比较，发现新的方法的加密次数、解密次数都只有基本的同态加密方案的一半，因此大大节省了计算时间。本文的基于区块链上的隐私数据安全共享机制步骤与文献[16]的新的同态加密算法步骤一致，因此本文引用了文献[16]里的同态加密算法，定义过程如下：

(1)将第三可信方生成密钥、加密、解密 3 个随机算法记作一个随即组（密钥生成 Key-Gen，加密 Enc，解密 Dec）；

(2)Key-Gen：生成两个等长的素数 p,q，计算 $n = pq$， $\lambda = lcm(p-1, q-1)$.公钥 pk=(n,1+n)、私钥 sk= λ；

(3)Enc: 加密方随机选择 $k \in Z_n, r_1 \in Z_n, r_2 \in Z_n$ ， m<n ，计算 $g_k = (1+n)^k \bmod n^2, c_1 = g_k^m r_1^n \bmod n^2, c_2 = g_k^m r_2^n \bmod n^2$；

(4)Dec:解密方执行解密计算：$m=\dfrac{L\left(c_1^{\lambda} \bmod n^2\right)}{L\left(c_2^{\lambda} \bmod n^2\right)} \bmod n$,其中，$L(u)=\dfrac{u-1}{n}, u \in Z_{n^2}^*$，

由 Carmichael 的理论可以证明出 $\dfrac{L\left(c_1^{\lambda} \bmod n^2\right)}{L\left(c_2^{\lambda} \bmod n^2\right)} \bmod n=m.$

4　针对公共管理大数据共享的应用举例

公共管理大数据主要的来源是两个，一个来自政府内部，比如政府搜集的各种资料；第二个来自由政府业务产生的各种数据，比如从机场安检。除了政府内部数据产生的公共管理相关的数据之外，互联网数据例如网民群体产生的微博数据等，在外部数据里扮演了非常重要的角色。在公共管理开源数据庞大的使用群体面前，数据的安全性以及数据隐私在数据共享时难以得到保障。公共管理部门将数据看作是重要的资产，将如何保护各种类型用户的数据看作关键。部分隐私程度高的数据只供给特定用户使用、部分政府数据只供给特定的研究机构使用、部分企业数据也无法做到完全公开。因此需要专门设计基于联盟区块链应对公共管理大数据的存储方法，确保数据之间的访问安全与隐私安全。本文所提出的基于区块链上的数据安全共享加密机制，从基于区块链技术对数据的检验性、基于区块链数据的公共管理大数据安全共享的机制上，通过研究区块链技术的去中心化、加密共享和分布式账本技术与同态加密技术对公共管理大数据安全共享的结合点，解决了数据共享时隐私泄露的难题。

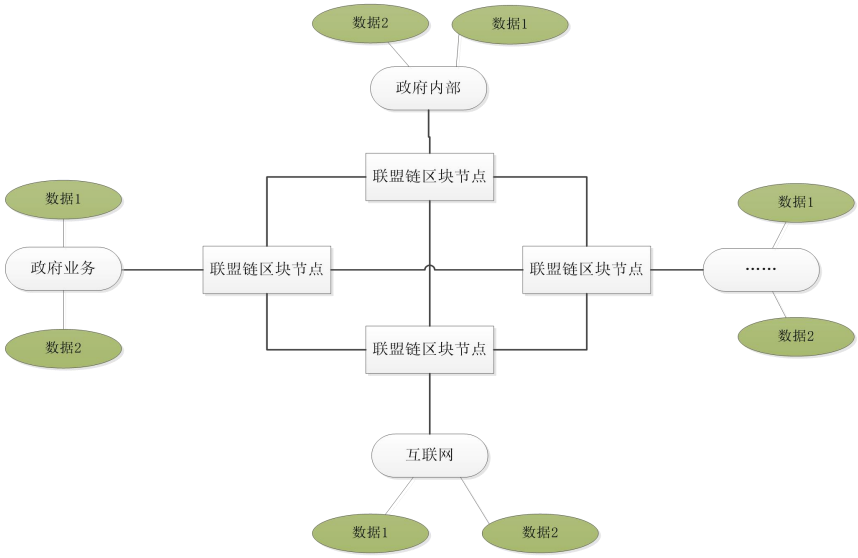

Fig.4　Schematic diagram of the public management big data alliance chain based on blockchain

图 4　基于区块链的公共管理大数据联盟链构造示意图

以公共管理大数据为例，数据共享分为两个层级，一个是联盟链内的数据安全共享，另一个是跨联盟链的数据安全共享。在采用本文的数据共享机制时首先对政府部门内部、政府部门和其他平台的终端和公众的数据共享需求进行前期实地调研或网络调查。在此基础上运用相关性分析等方法确定各部门的信息需求和最佳的信息流向，根据其需求确定此次共享的数据量，以及及时作好数据拆分。假如政府部门在需要共享一部分数据给其他部门以便各部门之间的沟通交流，首先内部确定需要共享的数据，其中是否包含隐私数据，拆分为这次需要共享的数据与不需要共享的数据两种数据类型，使用第三可信方全网生成的同态公钥加密成密文 X1、X2，再使用此次数据共享接收方的公钥再次加密需要分享的数据得密文 Y1。其次，利用区块链技术对政府和公众公共管理的相关数据资源进行统一的调配管理，由于区块链技术是一种特定数据库技术，可以保证数据安全共享策略和作为监测机制。数据的分享方将交易 X1、X2、Y1 三个密文发

送到区块链上，全网进行备份。最后，选取一个代表节点验证这次的交易是否成功，验证成功后将此次的交易记录在政府部门的区块链上进行备案，以便之后有需调出。数据的接收者收到区块链上的交易信息后，用自己的私钥解密密文 Y1，得知数据交易的记录，然后更新自己的数据。对于不同的层级数据共享机制，需要分成不同的链在区块链上进行，下图是部门 1 与部门 2 分别在联盟内与跨联盟链上的数据共享运行机制。在本文方案上，需求数据在正式共享时引进了同态加密技术保护数据的安全性，因此在保证数据的安全共享过程种，减少了隐私数据泄露的风险。

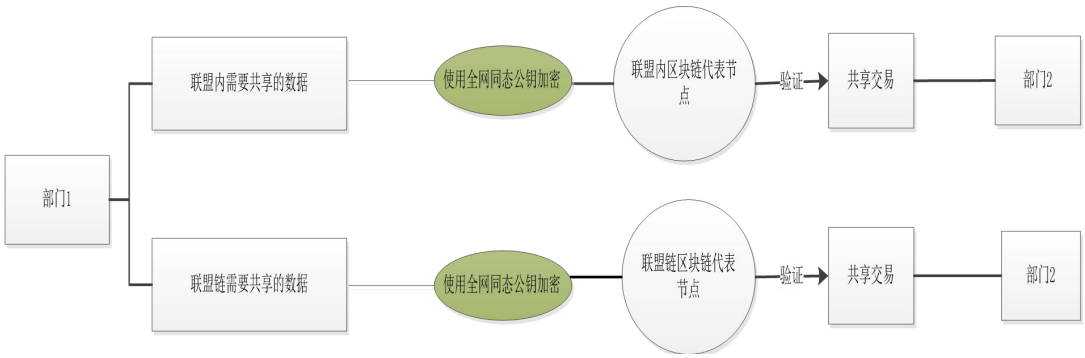

Fig.5　Common management data sharing mechanisms at different levels

图 5　不同层级的公共管理数据共享机制

5　总结

同态加密方案主要是加密隐私数据，而区块链技术的“分布式、去中心化”的明显特征，使得隐私数据安全共享具有较好的应用优势和前景。不少的学者在区块链技术与加密算法的结合应用方面给出了确保数据安全共享先进的研究。本文通过先分析数据共享在如今社会的影响性以及普及性，提出了结合基于区块链技术下数据共享的发展研究；再以区块链技术作为底层技术，提出了一种区块链技术下的隐私数据安全共享机制研究，结合结合了目前在区块上数据的共享过程以及在同态加密算法下的数隐私据共享保密方案，在经典的 Paillier 同态加密方案的基础上，结合本文的数据共享机制引入了一种变体的同态加密算法，在隐私数据安全共享方面给予了保障。本文提出的加密方案可以帮助隐私数据安全共享，以满足如今的共享经济的发展需求。只是，目前的研究还缺乏一定的实践支撑，这为本研究还需继续深入探讨奠定了基础。希望本文可以对数据安全共享时减少隐私数据的泄露提供一个好的借鉴，以便于未来的研究发展提供有益的启发。

参考文献：

[1] 孙晓燕. 科学数据共享行为的理论模型构建及测度实证研究[J]. 情报学报,2016, 35(10): 1062-1071.

[2] 庄倩, 何琳. 科学数据共享中科研人员共享行为的演化博弈分析[J]. 情报杂志,2015, 34(8): 152-157.

[3] 陈欣, 叶凤云, 汪传雷. 基于扎根理论的社会科学数据共享驱动因素研究[J].情报理论与实践, 2016, 39(12): 91-98.

[4] 何琳, 常颖聪. 科研人员数据共享意愿研究[J]. 图书与情报, 2014, (5):125-131.

[5] 张晋朝. 我国高校科研人员科学数据共享意愿研究[J]. 情报理论与实践, 2013,36(10): 25-30.

[6] LINEK S B, FECHER B, FRIESIKE S, et al. Data sharing as social dilemma:Influence of the researcher's personality[J]. Plos One, 2017, 12(8): e0183216

[7] WILLIAMSON K, KENNAN M A, JOHANSON G, et al. Data Sharing for theAdvancement of Science: Overcoming Barriers for Citizen Scientists[J]. Journal of the Association for Information Science and Technology, 2016, 67(10):2392-2403

[8] 董祥千, 郭兵, 沈艳,等. 一种高效安全的去中心化数据共享模型[J]. 计算机学报, 2018(5).

[9] 丁庆洋, 王秀利, 朱建明,等. 基于区块链的信息物理融合系统的信息安全保护框架[J]. 计算机科学, 2018, 45(2):32-39.

[10] 薛腾飞, 傅群超, 王枞,等. 基于区块链的医疗数据共享模型研究[J]. 自动化学报, 2017, 43(9):1555-1562.

[11] 李浪,余孝忠,杨娅琼,郑兰兰.同态加密研究进展综述[J].计算机应用研究,2015,32(11):3209-3214.

[12] 梁秀波, 李启雷, 尹可挺,等. 一种基于加法同态加密的区块链隐私保护方法:, CN 106549749 A[P]. 2017.

[13] Dennis R, Owen G. Rep on the block: A next generation reputation system based on the blockchain[C]// Internet Technology and Secured Transactions. IEEE, 2016:131-138.

[14] Rivest R. On databanks and privacy homomorphism[J]. Foundations of Secure Computation, 1978.

[15] 巩林明, 李顺东, 窦家维,等. 同态加密方案及安全两点直线计算协议[J]. 软件学报, 2017(12):3274-3292.

[16] Paillier P. Public-key cryptosystems based on composite degree residuosity classes[J]. Advances in Cryptology — Eurocrypt, 1999, 547(1):223--238.

[17] 袁勇,王飞跃.区块链技术发展现状与展望[J].自动化学报,2016,42(04):481-494.