Email:ycyk704@163.com　TEL:010-68382327　010-68382557

一类基于可监管区块链的公共安全信息共享平台方案设计*

王卯宁[1]，徐松艳[2]，段美姣[1]，贾恒越[1]
（1 中央财经大学信息学院　北京 100081；2 北京遥测技术研究所　北京 100076）

摘要：公共安全涉及到应急管理、供应链管理和医疗健康等领域，其数据共享平台对提供全方位、全过程的公共安全服务具有重要意义，尤其在当前的疫情背景下。但目前，由于涉及敏感数据的隐私保护，公共安全数据共享平台的架构设计一直面临着严峻的挑战。基于通过智能合约实现工作流协调和访问控制机制的设计思路，给出了一类基于可监管区块链的新型公共安全信息共享平台方案，并分析了其安全要求的可满足性，展示出依靠可监管区块链的验证机制和智能合约的自动执行，可以使得公共安全信息共享平台流程执行的正确性和数据的隐私需求得到满足。

关键词：公共安全；数据共享；区块链；智能合约；工作流
中图分类号：TP311.13; D63　**文献标识码：**A　**文章编号：**CN11-1780(2021)03-0008-06

The design of public safety data sharing platform based on permissioned blockchain

WANG Maoning[1], XU Songyan[2], DUAN Meijiao[1], JIA Hengyue[1]
（1. School of Information, Central University of Finance and Economics, Beijing 100081, China;
2. Beijing Research Institute of Telemetry, Beijing 100076, China）

Abstract: Public safety is related to emergency management, supply chain management and medical health, and its data sharing platform is of great significance to provide people with comprehensive public safety services, especially in the context of the current epidemic. However, due to the privacy protection of sensitive data, the architecture design of data sharing platform on public security has been facing challenges. To solve this problem, this paper presents a new design of public security data sharing platform based on permissioned blockchain. Its core idea is to realize the coordination workflow and access control mechanism by using smart contracts. Also, the satisfiability of the platform's security requirements is analyzed. The proposal of this scheme shows that relying on the verification mechanism of permissioned blockchain and the automatic execution of smart contracts, the correctness of process execution and the privacy requirements of data in the public safety information sharing platform can be met.

Key words: Public security; Data sharing; Blockchain; Smart contract; Workflow

引　言

公共安全，是指人群公共生活环境空间不受侵害并相对稳定的状态，它包括公民生命、财产、社会生活秩序和生态环境的安全，直接体现了与公民密切相关的公共安全利益的需要。作为公共管理的核心目标之一，公共安全一直是重要的研究课题。特别地，由于涉及到应急管理、供应链管理和医疗健康等领域，在当前的疫情背景下，对公共安全的研究显得尤为紧迫。其中，数据共享平台对提供全方位、全过程的公共安全数据服务和应用支撑具有重要意义——公共安全作为复杂的系统工程，必然无法在缺乏各行业、各部门大力协作建立信息共享的条件下实现发展。

然而，在公共安全领域，由于数据具有极高的隐私性，其共享不可避免地涉及到公共部门、私人部

*基金项目：国家重点研发计划（2017YFB1400700）；北京市自然科学基金（4194090）；国家自然科学基金（61702570，61907042）；中央财经大学青年教师发展基金（QJJ1823）；四川省教育厅人文社会科学重点研究基地科技金融与创业金融研究中心课题（JR2018-2）
收稿日期：2020-07-15　收修改稿日期：2020-09-04

门等多类主体的协作，在当前以“条”为主的垂直系统管理制度下，公共安全各部门的管理均局限于各自地区和领域，各组织、部门、制度之间已形成分割。数据资源具有价值，但其可复制性带来的难以确权问题，导致数据资源难以有效整合，出现了“数据孤岛”。此外，公共安全数据中涉及政府部门内部和政府部门之间的业务信息，对于公众往往又具有极高的敏感度、关注度和经济价值，不论是对公众的泄露，还是对其他非授权部门的泄露，一旦发生都将造成巨大的损失和严重的危害。当前尚无完善的体系来保障数据机密性和所有权，公共安全数据共享面临着严峻的挑战。

近年来，区块链技术出现，并以迅猛的发展趋势和广阔的应用前景吸引了各领域研究者的关注。目前，区块链技术已经在社会经济的多个领域中展露出了巨大的发展潜力，对金融、保险、会计、能源等领域面临的众多问题给出了变革性的解决方案。从直观概念来看，区块链技术有望成为解决公共安全数据共享障碍的一个有效途径，其本身蕴含的数据加密、时间戳、分布式共识和经济激励等手段，使得其具有高度透明、去中心化、集体维护、不可更改、匿名等性质，而这些正与公共安全数据共享所需要的公开、透明、协作等基本理念吻合；更进一步，区块链技术所强调的安全性，也正与公共安全数据共享以安全为前提的思路一致。

因此，能否利用区块链技术解决当前疫情背景下公共安全数据共享平台建设面临的痛点问题，是一个值得探索的问题，也是本文设计方案的出发点。

1　背景知识

1.1　区块链与可监管区块链

区块链[1-3]是一种分布式数据结构，它也被称为分布式账本，用来在网络成员之间复制和共享数据，并追溯网络参与者之间的每一次资源或资产交换。这些变化被记录到事务（交易记录）中，被收集并存放入有时间戳的链式数据块中，形成所谓的区块链。其链式构造的基础结构为：①每个块由其哈希值（即，应用于块内容的密码哈希函数返回的值）标识；②每个块包含链式数据块中其前面块的哈希值。此外，只有当网络参与者通过分布式共识协议验证交易有效时，才将交易录入数据块中。简单地说，如果大多数网络参与者诚实，则该协议是安全的。

在区块链中，事务（交易记录）必须根据预定义的规则进行验证。更进一步，验证过程衍生出了智能合约的概念，也就是一个预定义的编码交易验证计算的程序。支持智能合约的区块链可以被认为是通用的应用程序平台，目前最常用、最著名、最受支持的是以太坊[4]。在这个方向上的另一个相关倡议是 Hyperledger 超级账本项目[5]，这是一个跨行业的合作，旨在识别标准的开源智能合约以支持区块链和相关工具。

此外，从应用开发角度看，区块链实现方式有不同的分类，具体解释如下：

公有区块链。在这些区块链中，任何人都可以在没有特定身份的情况下加入网络。根据公有区块链的共识算法，可进一步将其分为两类：①无许可区块链。在这些区块链（如比特币）中，网络中的任何节点都可以参与共识算法，从而能够验证交易。②许可区块链。在这种类型的平台（例如 Ripple[6]、Stellar[7]）中，只有遵守指定规则的节点才能验证交易，从而成为共识算法的一部分。

私有区块链。在这样的区块链中，只有一部分节点被授权加入网络。其对单独的个人或实体开放，或者仅允许授权的节点加入网络并可根据权限查看信息，这样的区块链往往被用于机构间。与公共区块链类似，当任何节点可以参与共识算法（例如以太坊）时，它们可以进一步分为无权限区块链和许可区块链，其中，只有一部分节点被进一步授权验证交易（例如 Hyperledger 超级账本结构）。在这种情况下，分布式共识协议仅允许已授权节点创建新的区块，其中，节点权限由授权证明（证书）标记。

由于具有条件准入的机制，目前，私有区块链以及公有区块链中的许可区块链能够在保证数据无法篡改的前提下，响应监管机构的要求，被认为是“可监管区块链”。

1.2　公共安全数据共享业务模式

公共安全这一概念由来已久，其包含社会治安、交通安全、生活安全和生产安全等范畴。近年来，随着统计学理论与数据分析技术的发展，公共安全数据被收集和分析，逐步成为检验公共管理决策的重

要依据，作用于社会治理的各方面[8]。而数据共享成为更有效的数据分析的前提，何振[9]指出，公共安全数据共享有利于整合资源优势、优化权力配置，是行业协作的共同愿景；李明[10]指出，大数据时代背景下，提高公共安全信息共享能力，打破数据壁垒，跨领域、跨部门、跨地区的数据整合成为进一步对比与分析的必经之路。

然而，对公共安全领域数据共享进展现状的调研结果表明，当前公共安全数据共享存在着障碍。例如，何振[9]指出，各部门之间“数据割据”现象严重，使得巨量的数据分散在不同部门，政府数据整合能力不足，造成数据共享的瓶颈，成为大数据时代数据资源无法发挥潜在价值的原因之一。同时，研究者也正在探索障碍存在的原因，并尝试给出相应的对策。张春艳[11]指出，当前各部门、各行业、各地区的数据管理均局限于各自领域，而先进的技术工具支撑和完善的制度规则体系保障是公共安全数据协同共享治理的关键，呼吁政府管理者制定大数据国家战略规划，并在发展目标、发展原则、关键技术等方面做出顶层设计；黄全义[12]指出公共安全数据涉及政府不同部门和行业的数据，各部门/行业既需要共享这些数据，又需要按数据授权要求将不同数据和服务控制在不同的共享范围内，使得不该接触到特定数据的机构/人员无权看到该类数据，需要根据实际需求制定各类各项数据的共享方案，做到在自主、安全、可控下的共享，实现数据共享权限控制与管理功能。

目前，明确针对“公共安全数据安全共享”这一概念的、具体的技术方案和与之对应的管理策略研究尚不充分。但是，仍有一些涉及隐私性和所有权控制的数据管理方案值得参考。特别是近年来，“数据服务”这一概念被引入[13,14]，其核心思想是将数据所有者和数据服务提供者的权限分离。基于这一理念的扩展，EMEKCI[15]提出了基于数据分布的数据管理思路，可提供数据所有权限的均摊，同时避免了数据服务提供者过于集中和单一所引发的问题；SION[16]研究了数据查询隐私保护机制，即一个访问数据服务的数据请求者不向服务提供者泄露他确切的个人兴趣的方案，指出现有的方案均依赖于多个服务器的可用性，存在效率上的限制；SAMARATI[17]提出了通过在存放公开信息的公开目录中增加一个保护层的方法，该方法只允许授权访问数据的用户根据路径推导口令，从而可以安全、有效地发布信息。但由于需要在新的层中遵循与口令推导路径逆序方式的推导路径，作为一种技术策略，该方法不易被转化为平台管理机制。

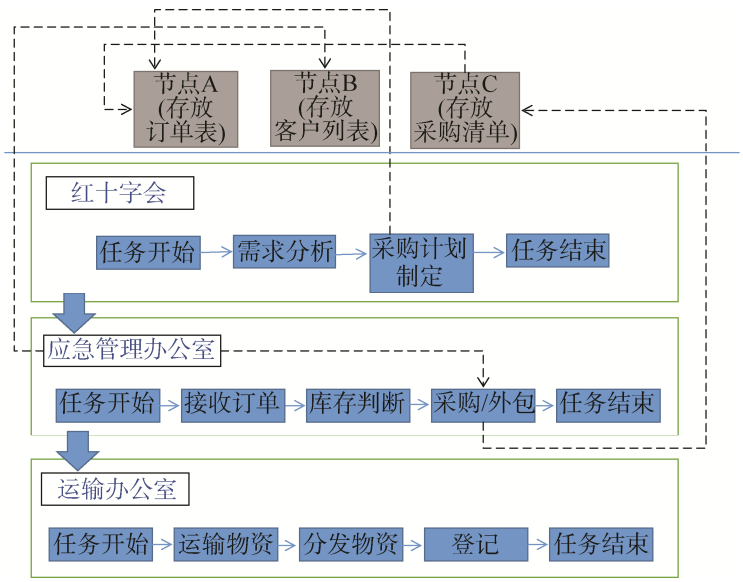

图 1　灾后重建工作流图

Fig. 1　The structure of post disaster reconstruction workflow

张鹏等人[18]考虑下面一个场景，并给出在云计算环境下的数据布局方法。由于具有典型性，本文的描述也基于该应用场景：某地发生灾害（疫情），在灾后重建的过程中，红十字会负责组织物资采购，该采购的工作流如图 1 所示。红十字会首先分析物资需求，然后根据分析结果制定采购计划。应急物资管理部门的负责人根据采购计划进行物资采购，然后通知灾区的运输部门把采购的物资运送到受灾地区。

2　方案设计

2.1　协作过程中的资源共享

在展示基于区块链的解决方案之前，在本节中，将更详细地说明协作过程的一般流程。一般来说，一系列机构 O 之间的协作过程可以建模为需要执行多个任务的工作流。每个任务 T 都必须由参与协作的机构之一执行，我们称之为执行者，表示为 T_{exec}。假设任务分配是在工作流执行开始之前完成的，并且

在工作流部署期间不能更改。任务 T 的执行可能需要对一组资源（表示为 T_{res}）执行不同的操作（例如，细化、查询、分析、可视化等）。除了自身的资源外，执行者 T_{exec} 可能还需要访问 O 中其他机构拥有的资源。对于每一个资源 $r \in T_{res}$，我们用 $O_r \in O$ 表示产生资源 r 的机构。

例 1：我们仍以上述红十字会调配应急物资的场景为例。该场景的目的是识别在给定的管辖区域内所需的应急物资、向应急管理办公室通报已确定的物资计划，然后应急管理办公室从登记册中检索供应商的联系人和物资储备信息，采购并授权供应商开始运输物资。这一过程意味着执行相关任务的机构（即红十字会、应急管理办公室、运输部门）与提供所需数据（如疫情评估、物资需求信息、供货商列表及商品储备、交通运力信息）的机构之间的合作。

这个过程的工作流模型如图 1 所示，其中第一个任务称为需求评估，由红十字会执行。为了执行这项任务，给定一个输入区域 X，需要从参与合作的不同组织（如当地医院、疾控中心）获取有关 X 区域疫情等级和物资缺乏状况的信息。如果需求评估任务返回的 X 地区疫情级别高于给定阈值，则制定采购计划，工作流将执行第二个和第三个任务。

更进一步，第二个任务称为紧急管理，由应急管理办公室执行，旨在根据采购计划，通过查询已登记供货商的服务信息（例如，供货商地理位置、运输条件、库存、联系人等），来查找能够为 X 区域内所需物资供货的供货商。返回的物资采购信息 ID 需要传递给第三个任务。

第三个任务，称为运输管理，由运输机构执行，该机构需从应急管理办公室检索相应的供货商联系信息和调配物资数量，并在取得授权后及时开始物资调配。

正如张鹏等人所指出的，上述任务中需要考虑隐私数据的存放[18,19]。当库存物资不足时，应急物资管理部门把订单外包给某工厂生产。这些外包的客户列表属于商业机密，应急物资管理部门在执行外包任务时，如果在公开数据源（例如云端或者开放型区块链上）输入这些数据，可能会导致间接地泄露这些数据。因此，在工作流架构设计时，需要同时考虑业务流程的完整性和用户数据的隐私性。

因此，为了支持工作流的执行，本文将协作过程的布局划分为两个主要的层：协调层（负责管理工作流任务的执行）和授权层（负责部署底层受控数据共享）。协调层必须通过向其执行者传递所需信息（即执行者必须执行哪些操作/服务以及可能的输入参数）来启动任务的执行，见图 2 中的实线步骤。例如，在例 1 中，协调层必须通过将 X 作为输入区域来与合作机构交互以调用其疫情等级评估服务。一旦任务被调用，协调层就会等待结果，并根据这些结果继续执行工作流。这可能意味着执行其他任务调用、循环或分支，直到达到最终状态。协调层必须与授权层密切合作。实际上，为了使任务执行者能够执行其操作，授权层必须设置适当的授权，使 T_{exec} 能够直接从所有者 O_r 的领域访问每个资源 $r \in T_{res}$，如图 2 虚线步骤所示。

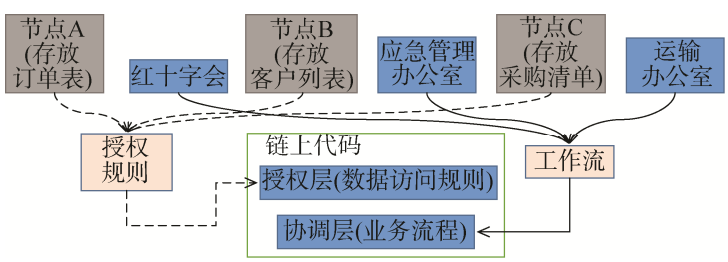

图 2　协作层、授权层与节点间的交互

Fig. 2　The structure of interaction among collaboration layer, authorization layer and other function nodes

2.2　基于区块链的数据共享工作流方案

结合可监管区块链具有的性质，为实现业务流程的完整性和用户数据的隐私保护，需要使得协作布局中的两层满足如下设计原则。

协调层：由于所涉及的组织之间可能缺乏信任，如何确保工作流的正确执行是一个难题。现有的方案往往通过将协调层委托给第三方来实现，第三方将完全控制工作流的执行（例如，任务、资源等）。然而，这可能会带来安全问题。例如，一个不诚实的第三方可以利用自己的地位来帮助一个机构盈利。此外，此类解决方案也会将整个过程暴露在一个独立的失败点。解决这种信任缺失的一个可行方法是利用区块链来支持安全的协作过程。区块链技术适用于此类场景，因为工作流可以由智能合约编码，由区块链执行和验证，通过分布式共识，它可以保证流程（即智能合约）的正确执行。

授权层：对于每个任务 T，此层的目的是部署一系列授权规则 T_{auth}，使执行者 T_{exec} 能够访问 T_{res} 中的资源。授权规则和相应的执行应当满足以下要求[1,20,21]，例如，临时激活原则（只能在任务执行期间允许访问 T_{res}）、动态资源指定原则（在工作流执行之前不能确认 T_{auth} 的条件是否满足，因此，T_{res} 中的资源可能是动态指定的）、最小特权原则（需要一种机制来检查 T_{exec} 是否要求更多的非必要资源来执行任务）、访问控制部署者原则（应当由数据所有者来设置其本地访问控制机制，以便当且仅当任务执行确实需要这些数据时，再将其发布给外部机构）。而基于智能合约高效的实时更新、准确执行、较低的人为干预风险、去中心化权威等特性，利用智能合约将授权规则配置在区块链中是合适的。

如下，本文展示如何在区块链工作流体系结构的设计中考虑上述需求，其主要思想是让协调层和授权层由 $\text{WF}_{\text{Engine}}$ 和 $\text{SC}_{T\,\text{invoke}}$ 两组智能合约控制。

不妨假设，在开始时，参与协作的机构同意一个协作工作流，并提交给一个名为 Deployer 的链外机构，由其负责创建定制 $\text{WF}_{\text{Engine}}$ 智能合约，之后，将获得的智能合约部署到区块链。对给定一个工作流 WF，$\text{WF}_{\text{Engine}}$ 智能合约被创建用来启动 WF，即调用初始化任务，然后根据该流决定下一个要调用的任务，直至达到最终状态。其中，$\text{WF}_{\text{Engine}}$ 的功能与任务的调用有关，而每个任务调用都被实现为一个独立的智能合约，即 $\text{SC}_{T\,\text{invoke}}$ 智能合约。这意味着要调用给定的任务 T，$\text{WF}_{\text{Engine}}$ 必须通过传递有关调用的信息（例如，关于 T_{exec} 的信息，可能的输入参数等）来创建和部署新的 $\text{SC}_{T\,\text{invoke}}$ 智能合约。

仍以图 2 中的工作流为例。为调用第一个任务 $T1$，$\text{WF}_{\text{Engine}}$ 创建一个智能合约 $\text{SC}_{T1\ \text{invoke}}$，其中 $T1_{\text{exec}}$ 是红十字会，输入参数是“area=X”。此时，$\text{SC}_{T1\ \text{invoke}}$ 的任务调用需要以下主要功能：①授权规则 $T1_{\text{auth}}$ 的部署和执行，其使得 $T1_{\text{exec}}$ 能够访问所需资源；②激活 $T1_{\text{exec}}$ 执行任务 $T1$ 的工作流；③规则 $T1_{\text{auth}}$ 的停用。其中，$\text{SC}_{T1\ \text{invoke}}$ 的主要步骤为①和③，目的是让授权规则和相关的执行条件直接配置在区块链中，即在 $\text{SC}_{T1\ \text{invoke}}$ 中实现。这样，通过利用区块链分布式共识机制，O_r 可以只用产生的交易记录作为正确执行授权的证据。

此外，节点 A、B、C 中的数据可能存放在传统的数据库管理系统中，而授权层中 $\text{SC}_{T\ \text{invoke}}$ 为区块链上的智能合约，在调用的过程中，需做额外的配置，现有的解决方案[22]主要包括将节点中的数据提前迁移到区块链上、在传统数据库管理系统上附加区块链特性、开发相应的兼容中间件等。

2.3　方案分析

由于智能合约 $\text{SC}_{T\,\text{invoke}}$ 只在任务 T 执行时才会被调用，而授权规则的配置是 $\text{SC}_{T\,\text{invoke}}$ 中的一步，并且合约包含相应授权规则的停用步骤，故只有在任务确实执行时才能访问和使用相应资源，即本方案可以满足临时激活原则的要求。

根据所考虑的场景，可能存在这样的情况：T_{exec} 应该被授权访问 $O_r \in O$ 的资源 r，而该资源 r 在任务执行之前没有确定。例如，应急管理办公室只能获取处于高风险地区的物资需求信息，而高风险地区的范围是动态变化的。本方案中，具体授权规则的确定是由 $\text{WF}_{\text{Engine}}$ 控制的，由于 $\text{WF}_{\text{Engine}}$ 本身就是一个智能合约，可以配置激活条件，故方案满足动态资源指定原则的要求。

由于对 T_{exec} 资源请求许可是在智能合约上进行的，因此，可以获得在工作流执行过程中哪些执行者访问过哪些资源。这使得后验检查（审计）具有透明度，以验证执行者的请求是否超出预期，从而防止违反最小特权原则。

由于本方案中，工作流是由参与协作的机构在配置 $\text{WF}_{\text{Engine}}$ 之前共同商定的，而 $\text{WF}_{\text{Engine}}$ 由链外机构配置，且其制定在信息对组织内部成员 O 公开的可监管区块链上，其具体的数据访问规则应当是由数据所有者 O_r 事先提供并许可的，故方案满足访问控制部署者原则的要求。

3　结束语

在本文中，我们展示了一类基于可监管区块链的公共安全信息共享平台方案设计，即如何利用区块链来保障在公共安全应用场景中，多个组织协作时工作流正确执行和隐私控制策略的实施。其核心思想是利用智能合约实现工作流协调和访问控制机制，并依靠智能合约执行的区块链验证来保证执行的正确性。

本文的工作可以从如下几个方面进行拓展。首先，本方案需要进行实验实施以验证其效率，可以选

择现有的成熟开发的许可区块链平台，如 Hyperledger Fabric 等；其次，对与本方案工作场景相关的安全属性和功能需求作进一步的形式化理论分析；再次，应当考虑将本方案部署在更广泛的应用场景时需要考虑的其他安全与性能问题。

参考文献

[1] CARMINATI B, FERRARI E, RONDANINI C. Blockchain as a platform for secure inter-organizational business processes[C]//2018 IEEE 4th International Conference on Collaboration and Internet Computing (CIC), IEEE, 2018: 122–129.

[2] 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(4): 481–493.
YUAN Yong, WANG Feiyue. Blockchain: the state of the art and future trends[J]. Acta Automatica Sinica, 2016, 42(4): 481–493.

[3] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[R]. Manubot, 2019.

[4] 闫莺. 以太坊技术详解与实战[M]. 机械工业出版社, 2018.

[5] ANDROULAKI E, BARGER A, BORTNIKOV V, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains[C]//Proceedings of the thirteenth EuroSys conference, 2018: 1–15.

[6] ARMKNECHT F, KARAME G O, MANDAL A, et al. Ripple: overview and outlook[C]//International Conference on Trust and Trustworthy Computing, Springer, Cham, 2015: 163–180.

[7] MAZIERES D. The stellar consensus protocol[J]. A Federated Model for Internet-level Consensus, 2015, July, 14.

[8] 汤志伟, 钟宗炬. 基于 CSSCI 的国内公共安全研究知识图谱分析[J]. 现代情报, 2017, 37(2): 119–125.
TANG Zhiwei, ZHONG Zongju. Research on knowledge map of public security literature in china based on CSSCI database[J]. Journal of Modern Information, 2017, 37(2): 119–125.

[9] 何振, 周芳检, 杨文. 大数据时代城市应急管理行业协作体制创新研究[J]. 湘潭大学学报(哲学社会科学版), 2016, 40(6): 26–31.
HE Zhen, ZHOU Fangjian, YANG Wen. On the research of industrial cooperation system innovation about city emergency management in big data era[J]. Journal of Xiangtan University(Philosophy and Social Sciences), 2016, 40(6): 26–31.

[10] 李明. 大数据技术与公共安全信息共享能力[J]. 电子政务, 2014(6): 10–19.
LI Ming. Big data technology and public safety information sharing capability[J]. E-Government, 2014(6): 10–19.

[11] 张春艳. 大数据时代的公共安全治理[J]. 国家行政学院学报, 2014(5):100–104.
ZHANG Chunyan. Public safety governance in the era of big data[J]. Journal of Chinese Academy of Governance, 2014(5): 100–104.

[12] 黄全义, 夏金超, 杨秀中,等. 城市公共安全大数据[J]. 地理空间信息, 2017, 15(7):1–5.
HUANG Quanyi, XIA Jinchao, YANG Xiuzhong, et al. Big data of urban public safety[J]. Geospatial Information, 2017, 15(7): 1–5.

[13] HACIGÜMÜS H, MEHROTRA S, IYER B. Providing database as a service[C]//International Conference on Data Engineering, 2002, Proceedings. IEEE, 2002: 29–38.

[14] MYKLETUN E, NARASIMHA M, TSUDIK G. Authentication and integrity in outsourced database[J]. Acm Transactions on Storage, 2006, 2(2): 107–138.

[15] EMEKCI F, AGRAWAL D, ABBADI A E. ABACUS: a distributed middleware for privacy preserving data sharing across private data warehouses[C]//Middleware 2005, ACM/IFIP/USENIX, International Middleware Conference, Grenoble, France, November 28 - December 2, 2005, Proceedings. DBLP, 2005: 21–41.

[16] SION R. Secure Data Outsourcing.[C]//International Conference on Very Large Data Bases, University of Vienna, Austria, September. DBLP, 2007: 1431–1432.

[17] DAMIANI E, VIMERCATI S D C D, FORESTI S, et al. Key management for multi-user encrypted databases[C]// ACM Workshop on Storage Security and Survivability. ACM, 2005:74–83.

[18] 张鹏, 王桂玲, 徐学辉. 云计算环境下适于工作流的数据布局方法[J]. 计算机研究与发展, 2013, 50(3): 636–647.
ZHANG Peng, WANG Guiling, XYU Xuehui. A data placement approach for workflow in cloud[J]. Journal of Computer Research and Development, 2013, 50(3): 636–647.

[19] 付永贵, 朱建明. 基于区块链的数据库访问控制机制设计[J]. 通信学报, 2020, 41(5): 130–140.
FU Yonggui, ZHU Jianming. Design for database access control mechanism based on blockchain[J]. Journal on Communications, 2020, 41(5): 130–140.

[20] CARMINATI B, RONDANINI C, FERRARI E. Confidential business process execution on blockchain[C]//2018 IEEE International Conference on Web Services (ICWS). IEEE, 2018: 58–65.

[21] RONDANINI C, CARMINATI B, DAIDONE F, et al. Blockchain-based controlled information sharing in inter-organizational workflows[C]// Submitted to the 2020 IEEE International Conference on Services Computing(SCC). IEEE, 2020.

[22] ZHU Y, ZHANG Z, JIN C, et al. Sebdb: Semantics empowered blockchain database[C]//2019 IEEE 35th International Conference on Data Engineering (ICDE). IEEE, 2019: 1820–1831.

[作者简介]

王卯宁 1987 年生，讲师，从事密码算法的分析与设计、区块链与数字货币方面的研究工作。

徐松艳 1978 年生，研究员，主要研究领域为武器系统信息安全分系统设计分析。

段美姣 1985 年生，讲师，从事物联网安全、数字取证技术、区块链技术方面的研究

贾恒越 1983 年生，讲师，计算机与信息安全系副主任，从事量子密码、量子数字货币等方面研究工作。