专题：区块链与数据共享

Blockchain and Data Sharing

客座编辑

魏凯（1981-），男，中国信息通信研究院云计算与大数据研究所部门主任，中国信息通信研究院互联网领域副主席，国际电信联盟分布式账本焦点组（ITU-T FG DLT）副主席，ITU-T SG16 Q21报告人，中国通信标准化协会TC1大数据与区块链工作组组长。牵头完成数据中心联盟大数据基准测试、可信区块链评测等标准和评测体系。主要研究方向为大数据和区块链相关技术与标准。

导读

区块链的概念来源于2008年中本聪发表的论文《比特币：一种点对点的电子现金系统》。在区块链系统中，各个参与者集体维护账本数据库，大家通过共识算法维护数据一致性，并以链式数据结构和复杂的加密技术确保数据不可篡改。这些设计与以往中心化的信息系统截然不同，代表着一种新的技术范式。区块链的出现，有望弥补传统网络技术在信任机制上的先天缺陷，为人们在数字世界进行数据共享、建立信任关系提供了一种便捷的方式。

当前，我国正在大力推动大数据战略实施。数据共享不充分，仍然是当前大数据与实体经济深度融合道路上最大的“拦路虎”。区块链的兴起，从技术角度为破解数据共享难题提出了一种新思路。本专题基于区块链的数据流通应用研究，收录了来自产学研专家的6篇文章，展示了国内在大数据与区块链结合方向的最新研究进展。

闫树等人的《区块链在数据流通中的应用》介绍了区块链如何利用其技术特性解决数据流通领域的痛点问题及应用案例。该论文在简要介绍区块链技术的基础上，阐述了利用区块链改造授权存证环节、进行数据溯源和实现智能合约的主要思路，进而梳理了实现数据流通的整体架构。在此基础上，给出了国外利用区块链进行数据流通的应用实例，并介绍了一些其他的数据流通新技术。

马小峰等人的《基于区块链的供应链金融服务平台》将目光聚焦在供应链金融服务的细分领域，介绍了一个基于联盟型区块链的供应链金融服务平台，提高了供应链数据流通的透明度、可追溯性和安全性。

蔡维德等人的《面向大数据的区块链在清算系统中的应用》介绍了区块链在清算系统中的应用实践，重点分析了大数据版区块链在清算过程中对复合交易进行拆解合并的架构设计，并从大数据分析层面提出对区块链上数据做风险决策与评估的潜在价值和重要意义。

钱卫宁等人的《区块链与分享型数据库》针对区块链在数据管理方面功能弱、性能低等问题进行了研究，对区块链和传统数据管理技术进行了对比，并对3个典型的金融领域以外的区块链应用进行了分析，探讨区块链上新的研究问题，并讨论面向特定领域应用研发分享型数据库系统（即支持核心业务，支撑分享经济业务模式，甚至本身也是以分享经济的方式实现的数据库）的必要性。

祝烈煌等人的《区块链交易隐私保护机制》对区块链数据流通方面不可规避的隐私保护问题进行了研究。论文分析了区块链交易数据面临的隐私泄露威胁，同时介绍以混币机制为代表的交易数据隐私保护机制，分析不同混币机制的优势与缺陷，并对数据隐私保护机制的未来发展方向进行了展望。

孙毅等人的《零知识证明应用到区块链中的技术挑战》则聚焦隐私保护中的关键技术——零知识证明，阐述并分析了零知识证明应用到区块链隐私保护方案中的技术挑战，给出了具有指导意义的解决方案。

本专题的目的是抛砖引玉，期待今后有更深入的成果呈现给读者。

区块链在数据流通中的应用

闫树，卿苏德，魏凯
中国信息通信研究院，北京 100191

摘要
大数据的流通是创造数据价值的关键一环，然而目前数据流通面临着诸多问题。区块链是一种分布式账本技术，具有去中心化和不可篡改特性，可以解决数据流通过程中的一些痛点问题。介绍了区块链技术的特性，阐述了利用区块链改造授权存证环节、进行数据溯源和实现智能合约的主要思路，梳理了实现数据流通的整体架构。在此基础上，给出了国外利用区块链进行数据流通的应用实例，并介绍了一些其他的数据流通新技术。

关键词
区块链；数据流通；智能合约

中图分类号：TP315　　文献标识码：A　　doi: 10.11959/j.issn.2096-0271.2018001

Application of blockchain in data circulation

YAN Shu, QING Sude, WEI Kai
China Academy of Information and Communications Technology, Beijing 100191, China

Abstract
Circulation of big data is a key link in the value creation of data, but there are numerous problems to be solved. Blockchain is a distributed ledger technology, which can be applied in data circulation by its decentralizing and immutable property. The main idea of authorized deposit certificate, data traceability and smart contract using blockchain was discussed, and the overall architecture of data circulation by blockchain was proposed. Finally, some applications and other data security solutions were introduced.

Key words
blockchain, data circulation, smart contract

1 引言

数据流通是指在数据提供方和数据需求方之间按照一定流通规则进行的以数据为对象的行为。这种情况下，数据脱离了原有使用场景，变更了使用目的。随着数据的资源价值逐渐得到认可以及大数据产业链结构日益完整，我国数据流通的需求也日益迫切。无论是共享还是交易，数据流通都使数据从数据产生端转移至数据应用端，优化了资源配置，正在成为释放数据价值的重要环节[1,2]。

根据数据使用的不同需求，流通的数据通常包括原始数据和加工处理后的衍生数据，涉及数据应用程序编程接口（application programming interface，API）、数据报告、原始数据分组、技术算法、数据应用等不同类型的数据资源商品。结合不同的数据使用需求，数据流通服务提供者通常采用不同的流通模式，如仅为提供方和需求方建立数据流通或服务关系的“中介型”服务；自主采集数据并对外销售的“采产销”型服务；对数据进一步加工处理，产生有价值的衍生数据或应用，并对外提供的“加工服务型”服务。在这些流通模式下数据提供方和数据需求方通常不是同一实体[3]①。

然而，我国数据流通，特别是交易产业数据流通，仍然面临着严重的问题，如数据隐私保护问题极其突出、数据权属问题需要得到准确界定、数据流通各环节标准缺乏统一共识、非法数据交易猖獗等。此外，随着《中华人民共和国网络安全法》的正式实施，贩卖非法数据正式入刑。在配套法规和标准不尽完善的情况下，许多企业为了规避风险，纷纷暂缓或缩小了数据流通产业规模。数据流通产业面临近年来最大的挑战，亟须通过新的技术应用提供新的保障。

近年来兴起的区块链技术，从技术角度对上述问题提供了一种解决思路。本文主要介绍区块链技术解决数据流通痛点中的几个关键应用场景，并梳理利用区块链实现数据流通的整体架构。

2 区块链技术概述

区块链是一种基于密码学原理构建的分布式共享数据库，其本质是通过去中心化和去信任的方式集体维护一个可靠数据库的技术方案。该技术方案允许系统内的所有节点都备份当前区块链的一个完整副本，每隔一段时间，系统选出这段时间记账最快最好的节点，该节点利用密码学技术计算和验证，将这段时间内的所有有效交易信息和当前区块链的“数字签名”记录到一个新区块上，并将新区块链接至当前区块链副本的末尾，形成新的区块链副本。区块链的任何变动都会依托整个系统的消息广播，实现全网区块链副本的更新。如上所述，区块链技术具备分布式对等、去信任、集体维护和无法篡改四大特点，因而与数据流通场景有着天然的契合度。

广义来讲，区块链是一种全新的分布式基础架构与计算范式。其利用块链式数据结构验证与存储数据、利用分布式节点共识算法生成和更新数据、利用密码学方式保证数据传输和访问安全、利用由自动化脚本代码组成的智能合约编程和操作数据。狭义来讲，区块链是按照时间顺序将数据区块依次连接形成的一种链式数据结构，是以密码学方法保证数据块的不可篡改和不可伪造的分布式账本。自区块链发展以来，全球金融体系率先对区块链技术进行各种试验与纠正。如今，区块链的发展已经可以通过分布式账本、不可篡改等特性，结合智能合约等技术，解决实际的复

① http://kns.cnki.net/kcms/detail/31.1289.TP.20171110.1508.004.html

杂业务场景。

区块链平台整体上可划分为网络层、共识层、数据层、智能合约层和应用层5个层次。为了实现数据的不可篡改性，区块链引入了以区块为单位的链式结构。不同区块链平台在数据结构的具体细节虽有差异，但整体上基本相同。以比特币为例，每个区块由区块头和区块体两部分组成，区块体中存放了自前一区块之后发生的多笔交易；区块头中存放了前块散列（preblockHash）、随机数（nonce）、Merkle根（Merkle root）等。区块链基于两种散列结构保障了数据的不可篡改性，即 Merkle 树和区块链表。图1描述了比特币的区块链数据结构[4]②。

3 利用区块链解决数据流通中的关键问题

通过区块链技术，可以在授权存在、数据溯源等数据流通的关键问题上进行改善，同时实现智能合约等新交易手段。

3.1 利用区块链改造授权存证环节

长期以来，由于数据流通方、加工方、使用方的分离，数据二次交易没有手段稽核及管控，无法实时校验授权真实性，数据交易授权在技术层面并没有过多进展，往往采用如图2所示的传统模式。在这种模式下，用户通过数据提供方或数据交易机构等中介机构进行一对一、单独的授权。

在传统模式下，授权存证可以被任意篡改，不具备公信力。由于需要相应责任认定条款，每个应用和数据源公司都需要单独签署协议。此外，查询授权记录需要单独开发接口，而这一点往往被忽略。由于授权和业务流程绑定，用户加入和退出都较为困难。

② http://kns.cnki.net/kcms/detail/11.1826.TP.20171115.2302.006.html

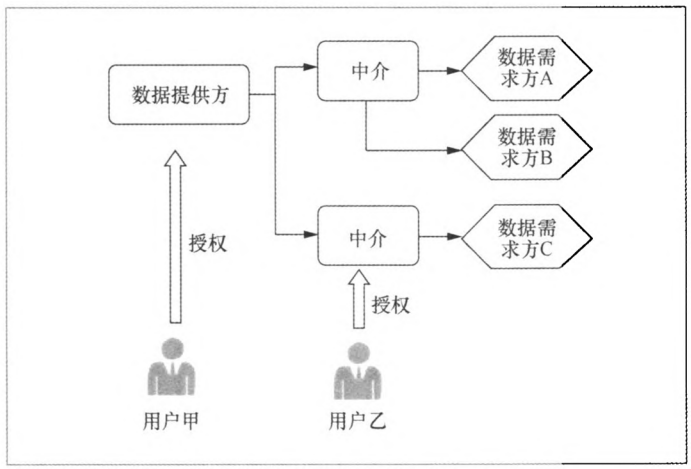

图 2 据交易用户授权存证的传统模式

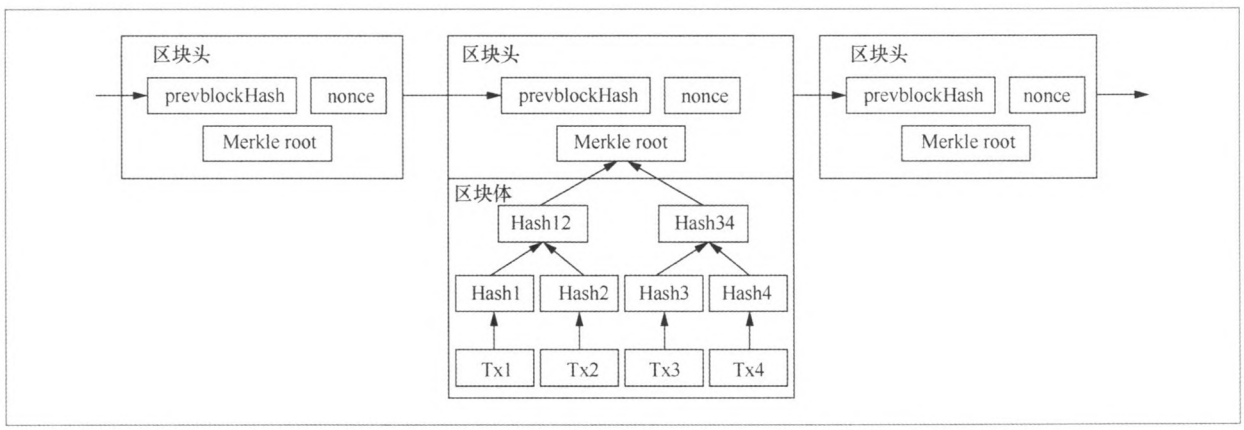

图 1 比特币的两种散列结构

区块链技术的发展使得这一领域产生了新的突破。在区块链模式下，完整的授权鉴权流程如图3所示。用户签署电子协议，授权给数据提供方相应权限。数据提供方首先通过应用系统本地存储凭证，进而将授权信息上传至授权信息链。应用系统执行链上代码，发起链上查询，并记录授权信息到区块。当数据需求方提交数据需求时，在链上发起鉴权交易，确认用户是否授权。接下来，链上验证节点返回授权信息，如确已授权，则返回相应数据。

区块链模式避免了传统模式的缺陷。任何节点可以记录授权信息，且不可更改。多方可以实时共享授权记录，查询效率较高。此外，授权与业务解耦，可随时加入和退出。

以中兴通讯股份有限公司为例，其基于区块链推出电子证照共享交换平台，利用区块链技术的平权、共建的特点，依据共建共享的原则实现全面数据归集；通过区块链发布可信任的证照信息，实现原始发布部门数字签名的不可篡改和数据可信；基于区块链技术的非对称加密特点，对每条信息进行单独加密（每条公民的信息有单独的解密私钥），防止信息泄露，加速推行“互联网+政务服务”，打造政务服务“一张网”，创新实现电子证照在市级范围内跨区域的信息归集、快速检索和结果应用，未来拓展到全省的电子证照共享交换平台，打造可信的省市级政府政务信息共享开放平台，保障政府各职能部门之间的数据共享开放安全。

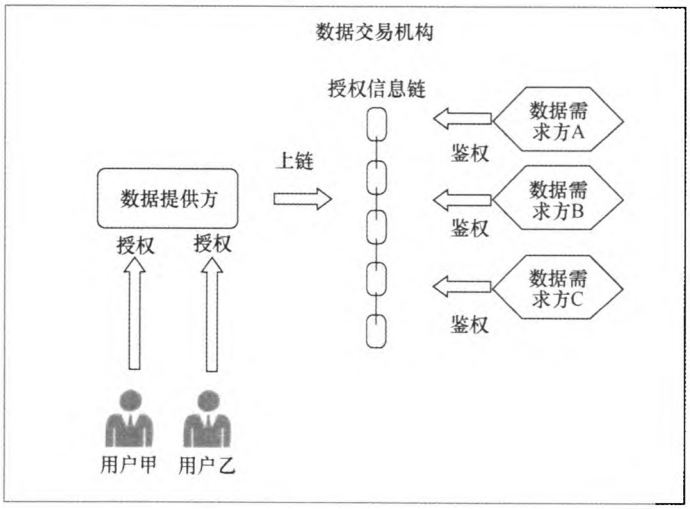

图 3 数据交易用户授权存证的区块链模式

3.2 利用区块链进行数据溯源

区块链技术的开放性、自治性、去中心化的特点非常适合数据交易（流通）溯源。目前，很多专家持有这样一种观点：数据+区块链=数据资产。区块链的价值就体现在对数据构造出了某种程度的“唯一性”。将带有唯一标识的数据附于区块链上进行交易，很自然地解决了数据难以溯源的问题。

区块链网络中多个参与计算的节点共同参与数据计算和记录，并且互相验证其信息有效性，既可进行信息防伪，又提供了可追溯路径。通过信息上链，各个区块的交易信息即构成完整的交易明细清单，不可篡改地记录了每笔交易的来龙去脉。当用户对某个区块的值有疑问时，可以准确方便地回溯交易记录，进而对历史交易记录进行判别[5]。

当前，基于区块链的供应链管控与溯源技术正在取得快速进展。例如，可以结合区块链、比特币相关技术和多重签名技术设计供应链管控和溯源方案。将供应链内部实体分为“人物实体”“产品实体”和“权限实体”，将分层钱包技术用于实体密钥的分配。构建基于分层钱包技术的树形结构编码体系，确立基于区块链交易的去中心化权限管控机制和物权转移信息记录与验证机制，从而提出利用区块链实现供应链管控与溯源的新思路。

例如，食品安全一直是困扰人们的一

大难题。以粮食为例，真正的五常大米年产不过100多万吨，而市场上销售五常大米的数量却超过1 500万吨，老百姓很难吃到真正的五常大米。2017年4月，智链(ChainNova)公司携手我国北方著名农场，运用基于Hyperledger Fabric 1.0的区块链技术和公钥基础设施(public key infrastructure, PKI)体系认证用户身份，打造了农业区块链应用。此应用对提交请求进行数字签名并上传至区块链上，从而保证数据真实不可篡改。同时，结合物联网、大数据等技术打通链上链下的全流程数据通道，实现了1 296万亩黑土地大米的追踪溯源与品质保障，将真正放心的高品质大米送到老百姓手中。

3.3 基于智能合约实现数据交易

智能合约由计算机科学家、加密大师尼克·萨博于1994年首次提出，是一个能够自动执行合约条款的计算机程序，即一个预先编好的程序代码，其对从外部获得的数据信息进行识别并判断。当满足程序设定的条件时，随即触发系统自动执行相应的合约条款，以此完成交易和智能资产的转移。然而，此概念提出后，因缺乏相应平台执行合约而处于被埋没的状态。

区块链技术的出现使智能合约重新被关注和研究。区块链技术中的分布式账本结构贯穿了业务层(如资产)、应用层(如智能合约)、中间件层(如分布式交易共识)和底层技术层(底层网络)。智能合约能够在应用层上进行存储、验证和执行，因此智能合约成为区块链技术应用的重要特征。

以数据交易为例，赋予资产一些代码并在区块链上运行，使其成为全网共享资源，再通过外部数据触发智能合约执行，以决定网络中数据资产的流通、分配或转移。智能合约的标的物并不限于数据，可以是汽车、房子等物质产权，也可以是股权、票据、数字货币等非物质产权。

智能合约不仅由代码定义，还由代码强制执行，因此智能合约完全自动且无法干预，合约双方无需彼此信任。这恰恰符合数据交易的需要。数据交易机构可以通过建立规则，并用代码表述形式代替合同，实现链上支付功能，提高自动化交易水平。

4 利用区块链实现数据流通的整体架构

利用区块链技术实现数据流通，可以从网络交换层、共识机制层、数据存储层、智能合约层和数据流通层5个层次进行梳理。这5个层次如图4所示。

在网络交换层，根据我国国家标准《信息系统安全等级保护基本要求》，非许可链(又称公有链)的技术架构在物理访问控制、网络安全保障、服务性能要求、系统可靠运行等方面并不适应国家的相关规定，因此，非许可链的架构并不适应信息系统的等级保护规定，只能采用许可链(又称联盟链或私有链)的方式进行部署，需要通过专线接入、构建虚拟私有网(virtual private network, VPN)等方式保证通信的安全可靠。在身份认证方面，使用行业类或者区域类的电子商务认证授权机构(CA认证)进行身份鉴权和接入控制，例如，做金融大数据交易的企业在进行接入时，需要通过中国人民银行下属的中国金融认证中心(China Financial Certification Authority, CFCA)的认证；在上海做大数据交易的机构进行接入时，需要通过上海市政府授权建立的上海市数字证书认证中心有限公司(SHECA)的认证等。整个网络是一种对等网络(peer-to-

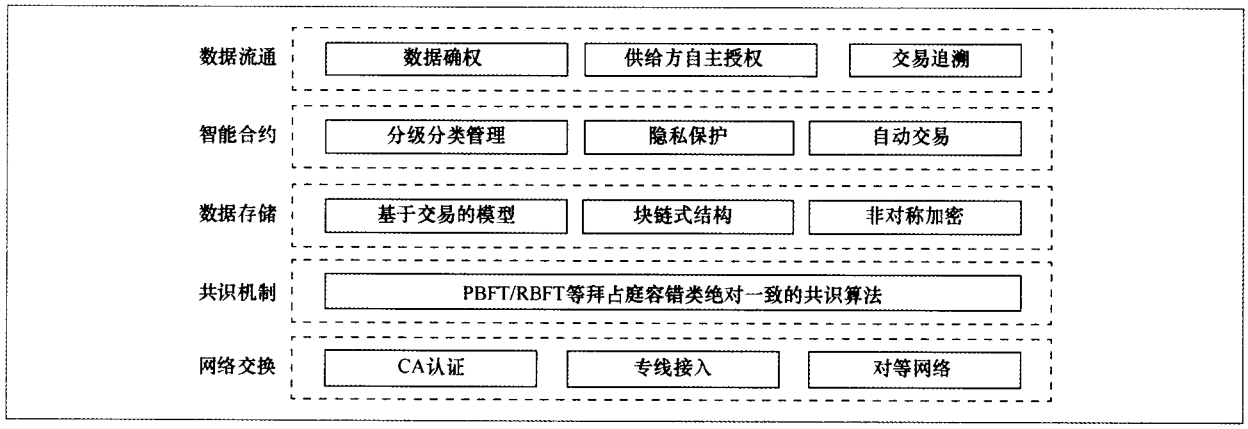

图4 区块链实现数据流通的5个层次

peer)，系统中多个节点的失效、退出和加入，甚至是恶意节点的存在，都不会影响整个系统运行的稳定性和安全性。

在共识机制层，区块链共识机制可以按照共识过程分为两类：第一类是概率一致的共识，工程学上最终确认，如工作量证明(proof of work，POW)机制、权益证明(proof of stake，POS)机制等；第二类是绝对一致之后再共识，共识即确认，如拜占庭容错(BFT)以及基于相关算法的变种(实用拜占庭容错(PBFT)算法等)。如前所述，在许可链的范畴中，尽可能采用绝对一致的共识算法。两类共识算法的比较见**表1**。

在数据存储层，每笔数据交易都要持续跟踪，采用不同于普通商业银行的复式记账法模型——基于交易的模型，即针对未花费交易输出(unspent transaction output，UTXO)模型，更适合数据交易的管控和溯源。并且，通过块链式数据结构实现环环相扣的历史交易信息，通过非对称密码学技术实现公私钥的加解密，有助于数据交易之前的数据确权和数据上链等操作。

在智能合约层，依靠智能合约在隔离沙箱中的独立执行和相互校对能力，可以通过代码编写精确表达、实现数据分级分类管理的权限控制，有助于实现多个政府委办局之间的层级映射，也有助于跨层级、跨部门、跨区域、跨平台、跨行业的多机构协作联动。在隐私保护方面，主要依托智能合约独立运行的沙箱环境，除了数据授权方和利益相关方，无人能够接触到相关数据，并且严格按照智能合约设置的数据查看权限进行数据访问，这从一定程度上保证了数据的隐私性。更多的隐私保护技术在后文会有更详细的描述。通过智能合约的自动执行衍生出数据的自动交易，有助于解决数据定价难、精准计费难、交易撮合难等诸多问题。

在数据流通层，依托网络交换层、共识机制层、数据存储层、智能合约层等相关机制，数据提供方相较于传统的数据流通平台，更容易对自己的数据进行加密后传输，方便实现数据的确权管理。数据流通平台面对加密后的数据，更容易自证清白，避免流通数据的泛滥复制。依托区块链系统的溯源功能，数据所有方可以跟踪数据的流通现状，并且数据的每次使用都需要数据所有方的授权验证，实现数据提供方对拥有数据的自主管控，数据需求方可以追溯数据的源头，确保数据分析的真实性，提升数据分析的精准性和有效性。

值得指出的是，为增强数据流通的可靠性和安全性，区块链在研发设计中可以

表1 共识算法对比

算法名称	最小节点数	容错率	简述	特点
PBFT	4	$f/(3f+1)$	可应对f个节点的丢弃响应、伪造数据、故意返回错误、对不同节点不同响应的欺诈行为	优点：共识即确认，交易确认时间短、效率高； 缺点：需要预知节点数量，去中心化程度不如POW
BFT-Raft	4	$f/(3f+1)$	在Raft算法基础上加入投票签名与请求、响应签名，不完全相信主节点数据，每个节点需要一个非主节点请求确认，可防止节点欺诈，易于理解实现	优点：共识即确认，交易确认时间短、效率高； 缺点：算法需要预知节点数量，去中心化程度不如POW
POW	1	依赖算法难度与参与节点运算能力	采用散列算法，使用多个变换的输入，暴力计算某个符合要求的散列值，并且散列值不小于256 bit，通过计算一个随机数，得出符合要求的散列，根据散列值不可逆的特点，除了暴力计算外，没有其他办法运算，所以如果获得符合要求的散列，则说明在概率上付出了对应的算力，从而证明节点确实做了某项工作，该算法在节点数越多的情况下欺诈的成本越高	优点：完全去中心化，节点自由进出； 缺点：暴力造成大量的资源浪费、共识达成的周期较长
POS	3	依赖算法难度与参与记账节点的运算能力及记账节点所占的权重	在POW基础上加入节点权重，引入代币作为权重依据，根据每个节点所占权重的比例和时间，等比例地降低POW难度，从而加快找随机数的速度	优点：减少参与验证和记账节点的数量，可加快共识周期； 缺点：依赖于代币
委任权益证明机制	3	依赖算法难度与参与记账节点的运算能力和记账节点所占的权重	在POS的基础上，每个节点根据权重，投票选出一定数量的节点，代替其进行验证和记账	优点：进一步减少验证和记账节点的数量，可以达到秒级的共识验证 缺点：依赖于代币

更加关注以下几点：一是选择正确的共识算法，依据数据流通对时效性的要求，综合考虑共识算法；二是选择合规的个人信息保护算法，发挥区块链的技术优势，严格进行个人信息保护；三是选择适合的区块链部署模式，依据数据流通的特点和安全性要求，以许可链为主，确定较为适宜的区块链部署模式；四是可以将加密算法与数据的分级分类机制有机结合，对不同级别、不同敏感度的数据采用不同成本的加密算法，从而整体提升数据流通效率。

5 区块链数据流通应用实例

区块链在电子病历数据流通共享等医疗健康领域的应用已经取得了重要进展。在美国，由国家卫生信息技术协调办公室（Office of the National Coordinator for Health Information Technology）主导的电子病历（electronic medical record，EMR）共享已经进入应用阶段，在此进行简要介绍[6,7]③。

EMR共享区块链模型具有较强的可扩展性。每个区块记录患者的唯一身份识别信息、经过加密的病历以及病历的时间戳。为改善数据通达效率，区块中还以标签形式记录了数据格式等元数据内容。所有医疗数据都存储于被称作数据湖（data lake）的数据库中，其可存储各种不同类型的数据（包括图像、文档等），这种存储是加密并结合数字签名技术的。数据湖中的数据在进行数据分析时具有极高的价值。

当医疗机构开出EMR时，会自动生成一个数字签名来验证开出机构的资格，

③ http://www.truevaluemetrics.org/DBpdfs/Technology/Blockchain/11-74-ablockchainforhealthcare.pdf

随后数据被加密传输至数据湖。同时，在EMR共享区块链上，由数据湖生成一个包含患者唯一身份识别信息的记录，并告知患者本人。其过程如图5所示。

上传后的数据在访问控制方面非常严格。用户可以决定谁能访问和修改相应的数据，并且可查阅到信息在何时被何人访问。

来自美国麻省理工学院的一些研究者还提出了利用区块链技术去中心化地处理EMR信息的全新系统，并命名为MedRec。数据研究者和公共卫生机构等利益相关者作为“挖矿者”参与网络，并获取经过脱敏、用于科研的相关卫生数据。这种“挖矿”过程可认为是一种POW机制，也可以看作“比特币”机制在数据流通中的应用尝试。

事实上，由于欧盟《一般数据保护条例（European General Data Protection Regulation，GDPR）》的公布，数据保护的要求越来越高，导致更多的科研机构和企业开始探索利用区块链实现数据流通，区块链与云计算和安全审计等技术的结合受到广泛关注。

6 其他数据安全解决方案

区块链作为一种共享账本技术，要做到数据隔离，还需要与其他数据安全技术组合使用，如零知识证明（zero-knowledge proof）、安全多方计算（secure multi-party computation，SMC）等。

6.1 零知识证明

零知识证明是由Goldwasser等人在20世纪80年代初提出的。它指的是证明者能够在不向验证者提供任何有用信息的情况下，使验证者相信某个论断是正确的。

证明方和验证方拥有相同的某一个函数或一系列的数值。零知识证明的一般过程如下：

- 证明方向验证方发送满足一定条件的随机值，这个随机值称为“承诺”；
- 验证方向证明方发送满足一定条件的随机值，这个随机值称为“挑战”；
- 证明方执行一个秘密的计算，并将结果发送给验证方，这个结果称为“响应”；
- 验证方对“响应”进行验证，如果验证失败，则表明证明方不具有其所谓的“知识”，并退出此过程。否则，继续从第一步开始，重复执行此过程t次。

如果每一次验证方均验证成功，则验证方相信证明方拥有某种知识。而且此过程中，验证方没有得到关于这个知识的一

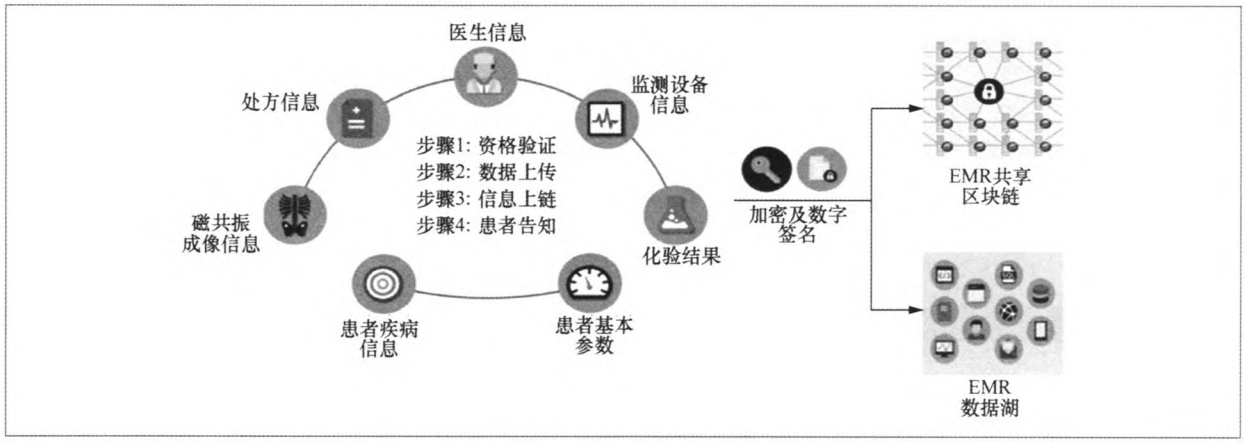

图 5 EMR 共享区块链及数据湖信息示意

点信息，成功地保护了证明方的隐私。

6.2 安全多方计算

安全多方计算用于解决一组互不信任的参与方之间保护隐私的协同计算问题，安全多方计算要确保输入的独立性、计算的正确性，同时不泄露输入值给参与方。通常，一个安全多方计算问题是指在一个分布式网络上计算基于任何输入的任何概率函数，每个输入方在这个分布式网络上都拥有一个输入，这个分布式网络要确保输入的独立性、计算的正确性，而且除了各自的输入外，不透露任何可用于推导其他输入和输出的信息[8]。

可以将安全多方计算简单地概括成如下数学模型：在一个分布式网络中，有n个互不信任的参与者$P_1,P_2,\cdots,P_n$，每个参与者P_i秘密输入x_i，他们需要共同执行函数$F:(x_1,x_2,\cdots,x_n)\rightarrow(y_1,y_2,\cdots,y_n)$，其中$y_i$为$P_i$得到的相应输出。在函数$F$的计算过程中，要求任意参与者$P_i$（除$y_i$外）均不能够得到其他参与者$P_j(j\neq i)$的任何输入信息。

一般化的安全多方计算协议，由于其计算任务的无关性（可以计算任意的功能函数），不需要再考虑特定的安全属性及外部运行环境，所以对现阶段复杂应用的安全保障具有得天独厚的优势。

7 结束语

区块链通过建立一组公共账本，由网络中所有用户共同记录，保证信息的真实性与不可篡改性。这些特性使得区块链有望成为破解数据流通难题的有效工具。然而，区块链的性能瓶颈和延迟性问题也愈发明显。除了技术方面的问题，其搭建成本以及与现有系统的融合性都成为制约其未来发展的因素。未来区块链能否在数据流通中发挥更大的作用，还取决于很多因素。

参考文献:

[1] 安庆文. 基于区块链的去中心化交易关键技术研究及应用[D]. 上海：东华大学，2017.
AN Q W. Research and applications on the key techniques of decentralized transaction based on blockchain[D]. Shanghai: Donghua University, 2017.

[2] 刘德林. 区块链智能合约技术在金融领域的研发应用现状、问题及建议[J]. 海南金融，2016(10)：27-31.
LIU D L. Current situation, problems and suggestions for the development and application of the block chain smart contract technology in financial field[J]. Hainan Finance, 2016(10): 27-31.

[3] 刘倩. 利用区块链技术健全大数据价值流通体系[N]. 中国信息化周报，2017-09-11.
LIU Q. Using block chain to improve the value circulation system of big data[N]. China Information Weekly, 2017-09-11.

[4] 尹冠乔. 区块链技术发展现状及其潜在问题文献综述[J]. 时代金融，2017(2)：299，301.
YIN G Q. Development and potential problems in block chain technology[J]. Times Finance, 2017(2): 299,301.

[5] 韩涵. 区块链渗入数据交易解决溯源与授权“痛点”[J]. 通信世界，2017(19)：53.
HAN H. Solving source tracing and authorization problems by block chain in data transaction[J]. Communications World, 2017(19): 53.

[6] ZYSKIND G, NATHAN O, ALEX. Decentralizing privacy: using blockchain to protect personal data[C]//The 2015 IEEE Security and Privacy Workshops, May 21-22, 2015, San Jose, USA. Washington, DC: IEEE Computer Society, 2015: 180-184.

[7] AZARIA A, EKBLAW A, VIEIRA T, et al. MedRec: using blockchain for medical data access and permission

management[C]// International Conference on Open and Big Data, August 22-24, 2016, Vienna, Austria. Washington, DC: IEEE Computer Society, 2016: 25-30.

[8] 蒋瀚，徐秋亮. 实用安全多方计算协议关键技术研究进展[J]. 计算机研究与发展，2015，52(10)：2247-2257.
JIANG H, XU Q L. Advances in key techniques of practical secure multi-party computation[J]. Journal of Computer Research and Development, 2015, 52(10): 2247-2257.

作者简介

闫树(1989-)，男，博士，中国信息通信研究院工程师，主要研究方向为数据交易与知识图谱。

卿苏德(1985-)，男，博士，中国信息通信研究院高级工程师，主要研究方向为区块链。

魏凯(1981-)，中国信息通信研究院云计算与大数据研究所部门主任，中国信息通信研究院互联网领域副主席，国际电信联盟分布式账本焦点组(ITU-T FG DLT)副主席，ITU-T SG16 Q21报告人，中国通信标准化协会TC1大数据与区块链工作组组长。牵头完成数据中心联盟大数据基准测试、可信区块链评测等标准和评测体系。主要研究方向为大数据和区块链相关技术与标准。

收稿日期：2017-12-05