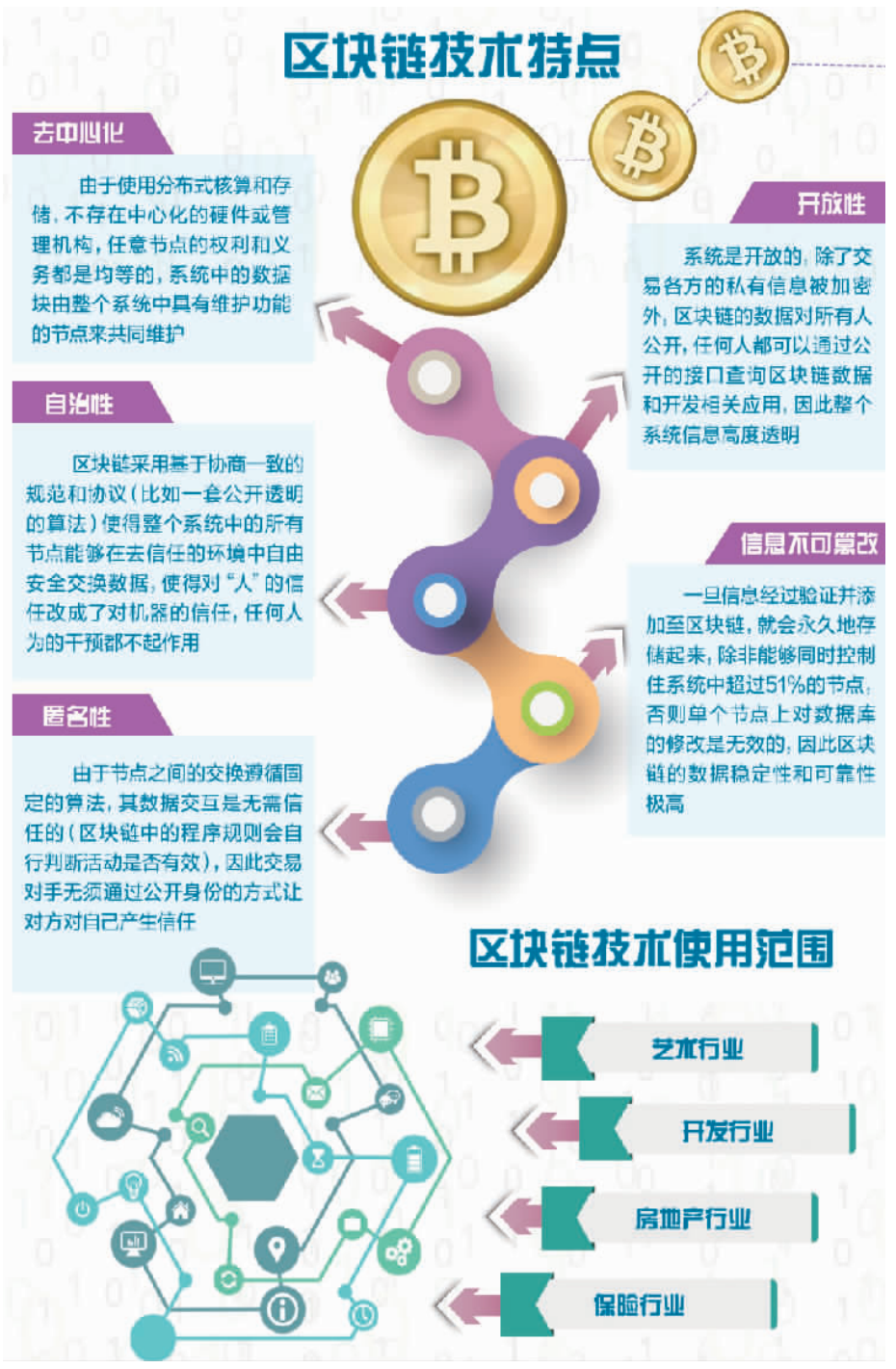
区块链+金融：让全世界为交易作证

本报记者 张 忱

热点追踪

近日，中国邮政储蓄银行与国际商业机器（中国）有限公司（IBM）宣布推出基于区块链的资产托管系统。此前，该系统已上线运行近3个月，完成了上百笔交易。这是区块链技术首次落地于银行核心业务系统。

区块链技术是新近的热门技术。但略显尴尬的是，区块链的研究热，实践冷：各种概念多如牛毛，相关研究连篇累牍，真正落地的应用却比较少。业内专家普遍认为，随着区块链技术的进步，区块链+金融将在应用领域实现更多突破。



无需中介的信任

在金融业务中，证明“我是我”，与交易对手建立相互间的信任，是比较麻烦的事情。比如，传统的托管业务往往需要资产委托方、资产管理方、资产托管方及投资顾问等多方参与。而且，各方都有自己的信息系统，单笔交易金额又大，从提出投资建议到真正的投资操作，参与方经常要通过传真、电话、邮件等方式审核、确认、协调，反复进行信用校验，才能最终达成一致，费时费力。

换句话说，在传统模式下，各参与方缺少一个共同信任的信息系统，无法在确保隐私性和安全性的同时，实现高效开放式合作，各种循环往复的繁冗确认过程不可避免。

而邮储银行推出的区块链解决方案实现了信息的多方实时共享，免去了重复信用校验的过程，能将原有业务环节缩短60%至80%，令信用交换更为高效。

效率提升的关键，就在于区块链技术具有不可篡改和加密认证的属性，可以确保交易双方在快速共享必要信息的同时，实现账户信息安全。这为解决金融行业需要同时满足开放性与安全性的难题，提供了理想方案。

那么，区块链到底是什么？区块链可以看作一个账本，一个可以让陌生人绕过中介建立信任的账本。

苏宁金融研究院高级研究员何广锋分析，个体进行信息交流和价值交换，如网络购物、银行存取钱等行为时，会产生大量的数据与信息，由专门的第三方机构（银行、支付宝等）或中介来记录和存储。这些可信赖的第三方或中介还会帮我们审核交易的真实性，构筑双方的信任。区块链的出现，直接颠覆了“可信赖的第三方”的地位，让人人都参与记账和交易行为认证，从而绕开特定的独立第三方记账人，实现交易全民记账。

具体到区块链的基本原理就是：每一个区块网络的参与者都是一个节点，所有的节点都保存了一套完整且相同的账本。账本中记录了全部历史账户信息及交易信息，任何一个节点想要发起一个交易行为，都需要将交易行为信息传递到区块网络中的所有节点，确保保存于所有节点上的账本都能准确更新并验证这笔交易行为。

通俗地说，这是让全世界为交易作证。

“如果有人试图制造欺诈交易，它的节点信息将无法和网络达成共识。因为，其账本内容与大多数人的账本不一致，故不会被大众认可。”何广锋说。

华创证券分析师华中炜认为，区块链通过去中心化的形式，实现了整个网络内的自证明功能，而不是传统上由中心化（如银行、交易中心等）的第三方机构进行统一的账簿更新和验证。也就是说，区块链技术中，双方无须第三方中介授信，即可达成交易。

那些绕不过去的坎

借助区块链技术，存储、验证等关键环节，都无需某个中心进行集中管理，交易各方的数据交换也无需以互信为基础。由于网络中的所有节点都可以扮演“监督者”的身份，任意两个节点之间建立连接都不用担心欺诈的问题。由此，信息可以作为资产非常方便地在没有中心的状态下快速转移。这实际上解决了金融交易中的很多痛点。

邮储银行行长吕家进表示：“区块链技术能够低成本地解决金融活动中的信任难题，将为多方交易带来前所未有的信任和信用的高效交换，具有推动金融业深刻变革的潜力。”

那么，为什么目前“区块链+金融”实际落地的应用依然有限，甚至有人戏称，区块链是雷声大，雨点小？

华中炜认为，区块链技术目前仍处在萌芽阶段。广泛应用之前，其仍然面临许多技术问题，如交易速度、确认流程及数据容量限制等。

北京航空航天大学数字社会与区块链实验室主任蔡维德表示，目前的区块链技术还无法满足很多种金融交易的速度和规模要求。几个国家的央行也对外宣称，区块链技术达不到央行系统的性能需求。“不是像某些人说的那样，区块链能一秒跑两三百次交易，在金融领域就够了。”蔡维德说。

除了技术性能有待提升，安全性能也仍有提升空间。由于区块链在全网的共享属性，以及采取分布式记账的方式，使得个人使用区块链技术时，可能面临隐私问题。

阳光保险助理总裁苏文力认为，区块链记录了客户的数据，需要确保客户的隐私安全。现阶段，区块链基础平台在该方面仍有不足，一些数据被明码存放，易被不良分子跟踪分析。为此，一些区块链应用开发者不将敏感数据放在区块链上，确保客户的利益不受损害。这也限制了一些非常适合采用区块链技术实现的场景应用。

最有希望的突破点

尽管目前并不完美，但业内人士认为，区块链技术发展速度很快，可以预见，区块链必在金融领域应用愈加广泛。票据、清算等领域可能成为“区块链+金融”应用的突破口。

国金证券分析师宁远贵认为，区块链发展初期主要在一些低频次、数据量小、价值小以及无中心的金融领域进行尝试，并率先在中介较多的无中心领域，比如股权交易、票据以及贷款等实现突破。因为中介使得交易成本提升，无中心让区块链的普及阻力大大降低。

招商证券分析师刘泽晶认为，区块链目前尚处技术探索期，直接从中心化体制跳跃至完全的去中心化体制或将面临安全和技术上的风险。短期内，实现区块链的“有限去中心化应用”将成为较大的可能，例如银行间的票据业务。

结合了区块链技术的数字票据将带来更加安全便捷的票据交易。数字票据可以实现票据价值传递的去中介化，并防范伪造、赖账等市场风险。在传统票据交易中，票据中介往往利用信息差进行撮合，区块链技术则可以实现点对点交易。由于区块链具有不可篡改和全网公开的特性，一旦交易，将不会存在赖账现象，从而避免了纸票“一票多卖”等问题。

另外，基于区块链的数字票据系统有分布式的特点，系统搭建和数据存储不需要中心服务器，省去了中心应用和接入系统的开发成本，降低了传统模式下系统的维护和优化成本。

支付清算是另一个可能的突破口。日前，瑞银集团及英国的巴克莱银行都在尝试运用区块链技术，以促进支付条件的完善。

当然，区块链技术在支付清算上的应用也并非遥不可及。一些区块链初创企业和合作机构已经提出一些全新的结算标准，比如，R3区块链联盟就已制定了可交互结算的标准。目前，全球已有超过40家大型银行和金融集团加入R3，其中包括中国平安保险。

在支付领域，区块链技术的优势在于它能够避开繁杂的系统，在付款人和收款人之间，创造更直接的付款流程。不管是境内转账还是跨境转账，这种方式都有着低价、迅速的特点，且无需中间手续费。

现阶段，商业贸易交易清算支付都要借助于银行。这种通过中介交易的传统方式，要经过开户行、对手行、央行和境外银行（代理行或本行境外分支机构）。在此过程中，每一个机构都拥有自身账务系统，彼此之间需要建立代理关系，需要有授信额度；每笔交易需要在本银行记录，还要与交易对手进行清算和对账等，导致交易速度慢、成本高。据统计，每年，因这些低效率问题，生态系统中的所有参与者共耗费1.6万亿美元。

刘泽晶表示，如果能基于区块链技术，构建一套通用的分布式银行间金融交易协议，为用户提供跨境、任意币种实时支付清算服务，跨境支付将会变得便捷和成本低廉。

不过，专家们也提醒，区块链应用的拓展也需要循序渐进。苏文力表示，“只有带给客户全新价值体验，区块链的应用才会有成功机会”。现有集中化的商业解决方案已为民众所熟悉，并能够为客户提供有效服务，如果不能为客户带来更多价值体验，不要勉强将其改造为去中心的区块链模式。

科谱

量子科技：带来无限可能

陈庆修

量子是光子、质子、中子、电子、介子等基本粒子的统称，是目前物理世界已知的最小基本微粒。日常生活中无处不在的光就由大量光量子组成。在量子力学中，科学家聚焦的是：在单个原子或次原子粒子尺度上，物质与能量的行为和相互作用。相较于宏观物理世界，量子有很多奇妙特性，诸如量子叠加和量子纠缠。其中，对通信最重要的影响是“量子纠缠”。量子信息学是量子力学与信息科学相结合的产物，它包括量子密码、量子通信、量子计算机等，近年来，在理论和实验上都取得了重大突破。

20世纪90年代，物理学家在理论上证明，对微观世界的物体而言，借助神奇的“量子纠缠”，可以将物质的未知量子态精确传送到遥远地点，而不用传送物质本身。将量子力学理论和信息技术结合，通过对光子、原子等微观粒子的精确操纵，信息编码、存储、传输等处理方式将会发生革命性变革。

由于一个量子单元的行为能瞬间影响另一个量子单元，从而改变被测量物质的状态，这一特性意味着，不可能实现对一个未知量子单元的精确复制。基于这一原理，科学家提出了量子密码的概念，也就是用具有量子态的物质作为密码。

量子密码是应用量子纠缠效应来进行信息的保密性传输，它的优点在于：不必在密码编辑上劳神费力，甚至根本不用常规密码，直接把信息以纠缠态方式发送，即可完美保密。原因是，当黑客闯入传输网络，光子束会出现紊乱，每个节点的探测器都会指出错误等级的增加，从而发出受干扰警报；发送与接收双方也会随机选取比较，全部匹配才会确认信息没有被窃听。这样一来，黑客就无法不留痕迹地闯入一个量子系统，甚至连尝试解码这一举动，都会导致量子密码系统改变原有状态。当然，即便有黑客成功拦截获得了一组密码信息的解码钥匙，也仅是乱码信息，而在完成这一举动的同时，也导致了密钥的变化。当合法的信息接收者检查钥匙时，则可以从量子态的改变中知道密码曾被截取过，一旦发现破绽，就会马上更换新的密钥。

量子密码的出现使密钥的安全性产生了全新变化。将量子密码应用于量子通信系统中，就成了量子保密通信。随着量子通信技术产业化和广域量子通信网络的实现，用不了太多时日，量子保密通信作为保障信息社会通信安全的关键技术，将会走向大规模应用——广泛应用于政治、经济、科技、金融等重要领域，为信息化社会提供基础的保密服务和最可靠的安全保障。

除了安全保密外，“神速”也是量子通信的另一大优势。传统通信的算法基础是0或1，而量子通信是量子单元，不仅含有0或1，还有0和1共存的状态，所有单元可同时完成逻辑运算，同时完成多重任务。量子计算机的这一特性，注定了量子通信的速度将比现在的通信速度大大提高。例如，4G网络延迟时间为50毫秒，无线电信号从火星传到地球要延迟十几分钟。而采用量子通信技术，不受传输距离影响，可消除延迟现象，实现“即时”通信。在未来，量子通信即时沟通的优势将大有用武之地。

显而易见，量子特性在信息领域中有着独特功用，在提高运算速度、确保信息安全、增大信息容量等方面，将突破现有信息系统的极限。量子通信可以从根本上杜绝窃密，确保信息安全，并能够极大提高信息处理速度。量子通信大规模推广应用后，“量子互联网”将顺理成章取代现如今的互联网。

而量子信息技术实用化的难点在于，对多粒子纠缠的操纵，这也是量子信息处理的核心物理资源。科学研究证明，要实现有实用价值的量子模拟机和量子计算机的基本功能，起码要实现几十到上百个量子比特的纠缠。目前，科学家仅能一次性将12种粒子纠缠起来；而量子计算机要实现商业化应用，至少需要将这一数字增加数十甚至上百倍。看来，量子通信的阶段性成果触手可及，而有决定性意义的成果还需再接再厉！

当然，量子理论的应用远超计算和通信领域，量子科学带来无限可能。正如爱因斯坦所说：“我们现在所看到的只是一个尚未完全理解的真正实体的局部。”通过量子理论，人类将有机会在微观和宏观世界之间架设桥梁。

总之，利用量子理论来变革信息技术，有望实现对信息处理能力的革命性突破，量子计算机和量子通信不只存在于科幻小说中，而是越来越接近现实世界。量子科技在推动人类社会文明进步方面将发挥颠覆性作用，要进一步创新技术和变革理念，以更好地操控多粒子纠缠，进而推动量子产业发展壮大。

本报记者 杜 芳

自打去年8月赤道中东太平洋拉尼娜状态诞生以来，专家根据监测数据推断有可能形成一次拉尼娜事件，从而导致偏冷的冬季。但是，人们从2016年等到了2017年，拉尼娜事件仍旧迟迟不来，暖冬依旧持续。2月7日，据国家气候中心最新监测结果，2016/2017年冬季拉尼娜事件确认未能正式形成。这表明赤道中东太平洋拉尼娜状态持续了4个月，终于未能达到连续5个月的基本判定指标，从而宣告冷水过程止步在拉尼娜状态。

拉尼娜是指发生在赤道中东太平洋海水大范围持续异常偏冷的现象。依据中国气象局最新修订的《厄尔尼诺/拉尼娜事件监测业务规定》，当关键区（尼诺3.4区）海表温度距平指数三个月滑动平均值低出同期0.5℃时，即进入拉尼娜状态，持续5个月以上，便形成一次拉尼娜事件。

自2016年8月进入拉尼娜状态以来，赤道中东太平洋冷海温持续平稳发展，但在秋季后冷海温范围缩小，强度减弱。国家气候中心监测显示，自2016年11月以来，拉尼娜状态开始明显减弱，11月、12月和2017年1月连续3个月的月平均尼诺3.4指数分别为-0.55℃、-0.42℃和-0.33℃。根据计算，拉尼娜状态仅持续了4个月，未能满足监测所需基本条件，不能形成一次拉尼娜事件。

在茫茫大海度过一生的拉尼娜，究竟依靠谁在补给能量呢？专家介绍，拉尼娜的原动力是信风和冷水。信风使大量暖水被吹送到赤道西太平洋地区，在赤道东太平洋地区暖水被刮走，主要靠海面以下的冷水进行补充。当信风加强时，赤道东太平洋深层海水上翻现象更加剧烈，导致海表温度异常偏低。这使得气流在赤道太平洋东部下沉，而气流在西部的上升运动更为加剧，有利于信风加强，引发拉尼娜现象。

此次拉尼娜事件之所以没有形成，国家气候中心气候服务首席专家周兵认为原因有二：首先，冬季拉尼娜所乘之风并不给力，即由东吹向西的信风太过弱势，使东太平洋的冷水上翻不足，导致拉尼娜持续“低迷”。还有一个重要原因是全球变暖，尤其是全球海表温度的变暖趋势十分明显，这使暖水事件易于达标，而对冷水事件比较不利，导致近年来拉尼娜事件与厄尔尼诺形成不对称性。

此外，“拉尼娜事件出局”与“冬季可能偏冷出局”几乎有一定的联系，今年我国冬季异常偏暖，主要原因是东亚冬季风偏弱，冷空气过程偏少、影响范围偏北所致。

国家气候中心预计，2017年后冬至春季，赤道中东太平洋仍将继续维持正常状态。值得注意的是，不同国家或机构因采用不同的资料或数据分析技术，可能会得出不同结果。国家气候中心表示，正密切关注赤道中东太平洋海表温度的变化以及它对冬季气候的影响，将及时提供信息服务。

稻瘟病研究获重大突破：

作物“杀手”有望攻克

本报讯 记者沈则瑾报道：我国科学家日前在广谱和持久抗稻瘟病机制上取得重大突破，相关研究论文已在《Science》上在线发表。这项研究成果不仅在理论上扩展了植物免疫与抗病性机制的认识，也为作物抗病育种提供了有效新工具。

稻瘟病由真菌引起，广泛侵染水稻、小麦等禾本科作物，被列为十大真菌病害之首，全球所有水稻产区都受其危害，严重时可导致颗粒无收。据估计，我国每年因稻瘟病发病直接损失稻谷约30亿公斤。因此，发掘新的抗病资源，选育广谱抗病新品种，成为迫切需求。2008年起，我国水稻新品种审定实行稻瘟病抗性的“一票否决”制。

为解决这一困扰植物病理和育种界的瓶颈问题，2002年起，中科院上海植物生理生态研究所的何祖华团队，经过不懈努力，鉴定出一个抗稻瘟病新位点Pigm——具有广谱和持久的抗瘟性。

随后，何祖华团队又用了10年时间，系统解析了这个新位点的功能机制。他们研究发现，Pigm位点有2个基因在起作用：一个抗病但降低产量，一个不抗病但增加产量。这两个基因不能分开，采用新的遗传方式调控基因表达和蛋白互作，可以达到广谱抗病与产量平衡，也使病原菌不能进化破坏水稻的抗病性。

新基因位点Pigm自发掘以来，已被广泛应用于我国水稻抗病育种。因此，这项研究不仅在理论上扩展了植物免疫与抗病性机制的认识，也为作物抗病育种提供了有效的新工具。

图为感染稻瘟病的稻苗。 （资料图片）

本版编辑 郎 冰 周明阳
联系邮箱 jjrbxzh@163.com