

研究报告

2018 年第 3 期

2018.1.10

执笔人：刘新

邮箱：liuxin@icbc.com.cn

金融科技系列研究之三

分布式账本技术

在支付清算领域的应用前景研究

要点

- 从广义角度来看，分布式账本技术是点对点网络、分布式数据存储、加密技术等多种技术要素的组合，具备存储、记录和转移数字资产的能力。分布式账本技术可以降低交易复杂性（尤其在多方清算及跨境支付领域）、提高端到端处理效率、降低跨多个基础设施的交易对账需求、提高交易记录的透明度和不可篡改性、提高网络弹性，未来在跨境支付、普惠金融、证券和衍生品交易等领域的应用前景广阔。
- 分布式账本技术的开发和应用仍处于起步阶段，目前面临商业、技术、金融、风险管理等四大类挑战。我行可采取成立实验室独立研发、与技术公司开展合作、成立联盟、支持创业公司项目等策略推进分布式账本技术的研究和应用。

重要声明：本报告中的原始数据来源于官方统计机构和市场研究机构已公开的资料，但不保证所载信息的准确性和完整性。本报告不代表研究人员所在机构的观点和意见，不构成对阅读者的任何投资建议。本报告（含标识和宣传语）的版权为中国工商银行城市金融研究所所有，仅供内部参阅，未经作者书面许可，任何机构和个人不得以任何形式翻版、复制、刊登、上网、引用或向其他人分发。

2017 年前三季度，我国各类支付系统共处理支付业务 557.52 亿笔，金额近 4000 万亿元，这些系统的安全、高效运行，对于维护金融市场平稳有序和金融稳定至关重要。分布式账本技术（Distributed Ledger Technology, 简称 DLT）被业界普遍认为能够改进支付、清算与结算流程，将对资金转移以及证券、商品和衍生品交易的清结算方式产生重要影响。考虑到分布式账本技术可能对支付清算体系及金融市场结构带来的变革性影响，本文拟对分布式账本技术及其在支付、清结算领域的应用机遇和面临的挑战等问题进行探析。

一、分布式账本技术的概念与特征

从严格意义上来说，分布式账本是由网络中各个节点共享的一种数据库，每一个参与者都可以获得一个真实账本的副本，通过公私钥以及签名进行访问和维护。从广义角度来看，分布式账本技术是点对点网络、分布式数据存储、加密技术等多种技术要素的组合，具备存储、记录和转移数字资产的能力。

（一）参与者可以通过节点实现点对点连接

在分布式账本技术中，通过节点之间相互连接，实现信息共享和验证。理论上，这种结构可以让每个拥有节点的用户，以点对点方式直接共享数据库管理责任。除了计算能力



之外，参与者在分布式账本中的参与能力还取决于账本的设计模式：**开放式系统**允许所有具备技术能力的实体运行节点，**封闭式系统**需满足一定额外标准（如流动性、信用等）才可运行节点。比特币等加密币属于开放式系统，金融行业设计的分布式账本一般属于封闭式系统。

（二）参与者可以在分布式账簿中发挥不同作用或功能

根据分布式账本技术参与者被允许发挥的作用或功能，可将分布式账本分为“无需许可”（permissionless）系统和“需经许可”（permissioned）系统，前者允许参与者开展全部活动，后者则对参与者活动施加一定限制，比如部分参与者仅能进行现有资产的交易，另一些参与者可以发行新资产；部分参与者仅能验证交易，另一些参与者可以将交易记录同步到账本中；部分参与者仅能读取账本数据，另一些参与者则可以写入数据。比特币等加密币属于“无需许可”系统，金融行业主要致力于“需经许可”系统的开发，以实现重要功能的有效控制。

（三）资产所有权可以存储在分布式账本中

分布式账本中的资产可以设计为多种形式，既可以在账本中发行和交易资产，也可以是账本外资产的表现形式。无论何种形式，资产的所有权信息都可以存储在账本中，并通

过账本维护全部参与者的所有权状态。分布式账本技术中的资产所有权人可以是银行或其他金融机构；如果在完全去中介的场景中，资产可以直接由家庭或企业持有。

（四）通过加密技术保障支付、清算与结算流程

通过加密技术的应用，分布式账本可以实现身份验证和数据加密功能。比如，在资产交易过程中，交易验证以公钥的加密技术为基础，交易发起方通过非共享的加密证书（即私钥）创建数字签名，作为交易验证方的参与者，通过算法和公钥对账本记录进行解密，验证资产权属的真实性。此外，加密技术可用于对账本中的交易信息进行加密，仅使某些参与者能够获得交易的具体信息。由于分布式账本技术一般要求在账本中公布交易记录，因此加密技术是实现必要隐私保护的重要工具。

（五）交易记录和所有权状态分布在账本的节点中

在分布式账本中，所有权和交易记录等信息可以分布在网络中的各个节点上。记录交易和所有权信息的账本，经参与者同意，作为共同账本在网络中共享。在账本的设计上，需规定哪些信息应当包含并在账本中共享，并规定哪些参与者能够在账本中读写信息。一般来说，即便所有节点都拥有账本的完整副本，仍可以通过技术对账本中的部分数据进行



加密，只有经授权的参与者才可以解密并读取基本信息。

（六）通过 API 提高分布式账本的可用性

API（Application Programming Interface，应用程序编程接口）是用于构建软件应用程序的一组例程、协议和工具，规定了软件要素之间的交互方式。在分布式账本技术中，API 可以实现新功能的添加或改进。比如，API 可以提供用户友好界面，令分布式账本技术更易于使用。随着使用不同协议的分布式账本技术的数量不断增长，API 在提高不同协议之间、协议和原有系统之间的可用性和互联互通性方面，将发挥重要作用。

（七）通过智能合约实现某些交易的自动执行

智能合约是基于一致同意的合同条款，用于自动执行预先设定条件的交易的编码程序。与传统合约类似，智能合约以参与者对条款的一致同意为基础。智能合约可与分布式账本技术结合，基于账本接收的信息进行自动执行。比如，一些公司正探索使用智能合约模拟公司债的发行，发债机构规定合同参数，如债券面值、期限和息票支付结构等，债券发行后，智能合约将自动进行所需的息票支付直到债券到期。

二、分布式账本在支付清算领域的应用前景

相对于传统的支付清算系统，分布式账本技术的七大特

征使其具有以下独特优势：降低复杂性（尤其在多方清算及跨境支付领域）；提高端到端处理效率，以及资产和资金的可用性；降低跨多个基础设施的交易对账需求；提高交易记录的透明度和不可篡改性；通过分布式数据管理，提高网络弹性。

分布式账本技术本质上与资产类型无关（asset-agnostic），理论上能够应用于所有类型资产的存储、记录和交易，潜在的应用领域十分广泛。

（一）跨境支付

目前的电子跨境支付是通过代理行模式，实现银行与银行之间的资金转移，一般涉及多重费用，且报文通信处理和结算时间较长。麦肯锡的一份报告显示，跨境支付的结算时间可长达五天，费用和结算时间的确定性不足，跨境支付中的成本一般会转嫁给终端用户。一些创业公司尝试通过分布式账本技术，减少跨境支付流程中的步骤，在对手方之间建立直接交互关系，缓解现有跨境支付模式中的摩擦。分布式账本技术的某些特性，比如跨时空共享账本的能力，可以减少跨境支付中所依赖的中介机构数量，让中小银行直接接入网络，从而降低成本并提高成本结构的透明度。

（二）普惠金融



高昂的账户服务费用和交通等间接成本，导致低收入群体在获取金融服务方面存在一定困难。通过分布式账本技术的应用，移动运营商等技术企业可以直接向终端用户提供低成本的金融服务，扩展传统银行机构未覆盖到的群体获取服务的渠道，为零售金融消费者降低成本，推动普惠金融发展。

（三）证券、商品和衍生品交易

分布式账本技术能够有效降低交易过程中的信息传输次数，提高操作速度和效率。此外，分布式账本技术能降低清算流程中的其他摩擦，比如跨多个账本的对账，使得市场参与者减少结算延迟和操作成本。通过分布式账本技术降低证券清结算流程中的摩擦，能够有效降低证券交易的中后台操作成本，如手工操作和机构间对账成本。目前，一些大型交易所正探索应用分布式账本技术，改进现有交易所模式中的交易后清结算流程。

三、分布式账本技术面临四大挑战

金融行业目前处于分布式账本技术研发的早期阶段，在技术成为支付、清算与结算领域实际应用的解决方案之前，仍有来自以下几方面的挑战需探讨解决。

（一）商业挑战

一是成本收益的权衡。在分布式账本技术应用中，挑战

之一是如何确定适当的应用场景，实现投资成本和潜在收益之间的平衡。此外，与现有或其他替代技术相比，分布式账本技术运营的长期成本是否具有比较优势，需结合具体应用案例进行对比评估。

二是网络效应的评估。网络效应是指网络中每一个新增用户都将提升现有用户的效益。由于缺乏足够数量的参与者，网络中早期应用者的净收益往往是负的，导致应用率较低。分布式账本技术在支付、清结算领域的广泛应用，取决于是否有足够数量的参与者采用该技术，许多参与者将网络效应作为影响技术应用和普及的关键因素。成立行业联盟，推动相关领域沟通合作，或将有助于解决网络效应带来的挑战。

（二）技术挑战

首先，分布式账本技术的可行性还有待进一步完善。一是可扩展性问题。我国的支付、清结算系统每天需处理数亿笔交易，共识算法和加密验证带来的延迟和处理笔数上的限制对系统运行效率带来一定挑战。此外，账本中不断添加的交易数据也对系统存储能力提出更高的要求。二是互联互通性问题。未来市场中可能同时存在多个分布式账本技术方案，部分原有系统可能也将继续运行。随着不同系统之间的



连接和应用的复杂程度不断提升，新旧系统并存客观上也增加了复杂性和碎片化程度，系统之间的互联互通性，将成为决定技术应用的重要因素。

第二，分布式账本技术的标准需要整合统一。对于增强不同系统的互联互通性而言，统一标准的重要性不言而喻。开放的行业标准有助于降低应用和整合成本，并确保分布式账本构建和访问方式的一致性。由于目前分布式账本技术的应用仍处于起步阶段，行业缺乏充分信息以建立适当的通用标准。不过，通过 API 的应用，机构可以在不大幅改变 IT 结构的前提下，实现分布式账本技术方案的运营，建立行业通用的开放 API 标准语言，这有助于降低进入分布式账本技术领域的门槛。

第三，对密钥和访问证书的有效管理尤为重要。与其他加密技术的应用不同，如果密钥或访问证书遗失或损坏，用户可能遭受无法挽回的财产损失，且没有救济和追索措施。维护私钥的私密性并实现公钥加密的安全性，是较为复杂并具有挑战性的任务。在密钥的使用和密钥管理系统的设计方面，需要相关组织和监管机构出台指引和最低要求，并将这些指引和要求应用于分布式账本技术方案。

第四，信息安全问题也值得关注。分布式账本的参与者

在账本中共享信息，且几乎不可能对信息进行更改，因此确保共享信息的正确性是系统运行的重要基础。如果许多参与者都可以在账本中进行记录，如何确保信息的正确性是一个不小的挑战。另一个挑战来自于确定哪些信息可以在账本中共享，特别是当参与者之间存在竞争关系时。参与者需就信息共享范围形成一致意见，并确定是否需中心化机构保管账本完整信息。此外，信息管理还需符合隐私方面法律法规的要求。

（三）金融挑战

首先，金融市场交易行为将受到影响。在当前的商业模式和社会组织架构下，陌生人由于无法相互信任，只有通过集中化的制度体系才能进行交易，中央银行、商业银行、清算机构是这一体系的重要参与者。分布式账本技术具有分布式数据存储、防篡改、加密技术保障等特点，为点对点的支付提供了可能和安全保障。由于减少了中间环节，分布式账本技术可以提高端到端处理速度，有望在转账、支付、境外汇款等领域大量使用，现有支付清算体系可能受到冲击，商业银行的中间业务收入可能受到冲击。

第二，金融中介的必要性问题。有观点认为，鉴于分布式账本技术在支付、清算与结算领域的独特优势，使用分布



式账本技术可以完全替代现有金融中介机构。笔者认为，分布式账本技术模式可能改变或削弱金融中介机构的部分作用，但市场仍存在对中介机构部分协调或中心化功能的需求，支付、清结算领域仍需必要的可信中介机构，以解决无法通过分布式账本技术解决的市场摩擦。长远来看，金融市场中中介机构的作用、职能和需求将会发生变化，但金融中介在资金供需双方的匹配、提供安全金融工具等方面，仍将发挥重要作用。

（四）风险管理挑战

法律、结算和操作性风险是支付、清结算领域的固有风险。根据目前金融市场结构，这些风险集中于银行、清算基础设施等机构。因此，上述机构成为风险管理的核心主体，政策和监管框架多以确保核心机构风险管理的有效性为目标设计。对任何分布式账本技术方案的应用和评估，需考虑其对支付、清结算流程造成的变化，是否会带来风险在市场主体间的传导，或导致市场整体风险的提高。

一是法律挑战。适用于支付、清结算领域的现有法律法规已较为完善，也将对分布式账本技术的具体应用方式和程度产生一定影响。在未来的应用场景中，应充分考虑法律框架可能发生的变化。比如账本中同步向参与者公布的记录，

其法律效力如何认定，是否可以作为确定基本义务和履行义务的依据。

二是治理挑战。透明、有效和可追责的治理机制是支付、清结算系统风险管理的重要组成部分。为确定风险管理的规则，分布式账本技术方案仍需健全治理机制。**开放和“无需许可”系统**可能需要分布式治理模式，使用共识算法确定网络协议或功能的更改。缺乏明确性、透明度和可预见性的治理机制，尤其在开放和“无需许可”的分布式账本中，将会对网络以及金融系统稳定性产生负面影响。相反，**封闭系统**，特别是对参与者的作用和功能进行区分的系统，可以创建较为中心化的治理结构，更类似于传统金融市场基础设施的治理模式，这种模式降低了责任和可追责性方面的不确定性，增加了治理结构调整的灵活性。

三是结算最终性挑战。金融交易中的一个核心风险是结算未如期发生的风险，导致结算未如期发生的原因包括对手方违约、操作问题或无法确定结算最终性。**分布式账本技术可能带来无法确定结算最终性的问题。**在目前的清结算模式下，结算最终性是一个法定或约定时点，交易双方及中介清算机构依据最终性的定义和时间，更新各自账本以实现结算、确定资产所有权并衡量和监控相关风险。在分布式账本



技术中，多个主体可以更新共享账本，并通过共识机制确定账本的特定状态，**结算最终性取决于概率**。通过概率确定最终性，法律责任可能难以分配或较为模糊，且这种不确定性对于参与者的资产负债表及其客户和债权人的权利都会产生影响。

四是操作挑战。系统弹性和安全性是操作风险管理中的核心要素。与传统中心化系统相比，分布式账本技术中的分布式数据存储，有望提供更高的系统弹性和数据完整性，账本中的某些节点产生风险，其他未受影响的节点可以维护账本的准确性，从而实现系统的持续运行。此外，利用分布式账本存储原有系统的数据备份副本，可以进一步加强对网络攻击的防御能力。但是，分布式账本技术存在端点安全性问题，其分布式结构使端点更易遭到攻击。分布式账本技术中的加密强度和密钥安全管理是另一个有待解决的重要问题。另外，随着风险和安全威胁不断变化发展，分布式账本系统安全管理流程和控制措施应持续对风险进行评估，传统的操作风险管理措施需进一步调整和修订，以适应分布式网络环境。

四、我行的应对之策

分布式账本技术为支付、清结算业务中的资产交易、信

息存储、身份管理等方式提供了全新的思路。借助点对点网络、节点之间的分布式公共账本以及加密技术等核心要素，分布式账本技术有望进一步提高市场运行效率，获得更为广泛的发展空间和应用场景。目前，分布式账本技术的开发和应用仍处于起步阶段，其对市场结构产生的影响，将随着研究应用的持续推进而逐渐清晰。鉴于分布式账本技术可能进一步推动金融市场结构的变化和调整，建议我行采取以下策略推进分布式账本技术的研究和应用。

一是成立实验室，独立研发。目前，摩根大通和高盛等全球性金融机构已着手部署和开发分布式账本技术，通过成立专业团队或创新实验室，进一步研究技术应用的潜在收益和成本。

二是与技术公司开展合作。目前，国内外已有技术公司独立进行分布式账本技术产品和服务的研发试验，比如以加密技术发行证券并在共享平台进行安全交易等技术解决方案。我行可以采取投资或直接与分布式账本技术领域的科技企业直接合作的方式，采取优势互补策略，共同推动技术应用研发。

三是成立联盟。以联盟形式开发分布式账本技术，参与者可以共同分摊相关成本和风险。此外，多边合作联盟有助



于推动共同账本操作标准的建立和概念验证项目的测试，获取先发优势。

四是支持创业公司项目。可以采取恰当的方式为相关领域的初创企业提供项目或赞助，包括提供资金、咨询服务或设备等，尝试在市场发展初期阶段主导一些优秀创业公司的发展方向。