内部资料　注意保存

中国社会科学院金融研究所支付清算研究中心
Research Center of Payment & Settlement, IFB

支付清算评论

2016 年第 1 期(总第 36 期)　　2016 年 1 月

目 录

如何看待 APPLE PAY 带来的挑战

日前，苹果公司 Apple Pay 移动支付服务正式登陆国内市场，引起了业界、媒体和“果粉”们的热议。虽然由于难以抵挡蜂拥而来的“尝鲜”热情，使得许多人的 IPHONE“绑卡”努力遇到困难，但其只要克服了“体验”阶段的“水土不服”，仍然会对国内移动支付市场带来新的冲击。

要理解 Apple Pay 的特点，需要从移动支付的技术内涵入手。移动支付也称为手机支付，就是允许用户使用其移动终端(通常是手机)对所消费的商品或服务进行账务支付的一种服务方式。单位或个人通过移动设备、互联网或者近距离传感直接或间接向银行金融机构发送支付指令产生货币支付与资金转移行为，从而实现移动支付功能。移动支付将终端设备、互联网、应用提供商以及金融机构相融合，为用户提供货币支付、缴费等金融业务。

我们知道，移动支付主要包括远程支付和近场支付。前者指通过移动网络，利用短信、GPRS 等空中接口，和后台支付系统建立连接，实现各种转账、消费等支付功能的支付方式。后者则是指通过具有近距离无线通讯技术的移动终端实现信息交互，进行货币资金转移的支付方式。

能够实现近场支付功能的技术手段包括 NFC 支付、蓝牙支付、红外线支付等，前者最为主流。在 NFC 支付中，又分为基于 TSM 的 SE-NFC 与 HCE-NFC 两种技术，前者需要在手机中存在一个安全芯片，后者基

于手机中的应用软件实现 NFC 卡模拟。

Apple Pay 则是典型的 SE-NFC 支付，而运用手机中的支付宝或微信支付进行网络购物时，则属于远程支付。当然，用手机支付宝或微信进行线下二维码扫码支付时，因为能够链接线上与线下，被人认为是介于二者之间的模式。

在 Apple Pay 进入之前，我国移动支付市场确实是“充满生机而躁动”的“一池春水”。一则，由于网络经济的快速增长、智能手机用户数量的大幅提升，使得我国成为全球范围的移动支付高增长区域，结合在经济金融转型中体现的市场成长性、监管对创新的容忍度较高，使得我国已经成为以电子支付为代表的新金融技术的实践“热土”。二则，在过去的 NFC 支付中，SE-NFC 遇到了产业链过长、硬件改造等带来的复杂利益协调问题，在推动中遭遇困难重重；银联已在重点推的云闪付则是基于 HCE 技术，但只能在安卓系统的手机上应用，苹果系统并不支持。三则，第三方支付的扫码支付由于流程更简单和便捷，因此迅速在移动支付领域占据了大量市场份额。虽然相关规则仍在完善中，监管层对消费者用手机扫商户二维码的潜在风险非常担忧，但也默认了商户用扫码枪扫消费者手机二维码的行为。

由此来看，Apple Pay 实际上通过整合产业链的合作格局，重启了 SE-NFC 的活力，并且将会搅动已有的移动支付市场格局。即便在短期内仍会遇到诸多挑战，但最终也会在国内移动支付市场中占据一席之地。

在深入探讨其优劣之前，还需要回答的是许多人的疑问，即：为

什么Apple Pay在全球发展缓慢，在美国也谈不上多么成功？例如，Info scout的追踪数据发现从2014年11月到2015年11月，在美国可以使用Apple Pay的交易中，苹果支付的所占比例反而出现了下滑,尤其在去年美国黑色星期五期间,一项涉及30万人的调查显示：Apple Pay在所有可用交易中所占份额只有2.5%，较一年前刚推出时明显下滑。事实上，发达经济体由于拥有较为完善的卡基支付体系，且有大量的非银行机构也可发行信用卡或预付卡,加上个人支票仍然大行其道，这使得其移动支付增速相较新兴经济体并不突出，甚至更低。此外，支付消费者的支付习惯路径依赖性、更严格的监管、多元化的竞争也都使得Apple Pay难以获得爆发式增长。

在我国，Apple Pay拥有的一些比较优势与特点，或许使其能够获得更多的发展潜力。一是从客户角度看，当绑卡等初始设定完成之后，其在具体的支付步骤上确实能够缩短支付动作，即便是短短的一两步节省，在愈加追求快速便捷的支付时代，都能够带来消费者体验的更加偏好。应该说，APPLE在整合NFC的软硬件协同与客户体验方面,确实有了重要的突破。同时,APPLE所一贯追求和体现的安全性，以及背后的安全机制 Tokenization，也使得Apple Pay更让消费者放心。

二是从行业和监管角度看，Apple Pay并没有改变现有的银行卡跨行转接清算的“四方模式”，而是在原有利益格局中寻求实现共赢的切入点，相对而言与银行、卡组组能够找到更多“共同语言”。同时，虽然在事实上挑战了第三方支付巨头隐形的支付转接清算“三方

模式”，但后者的主要阵地仍在线上，线下本来就是增长潜力巨大的前沿，促进竞争和行业“大战”，反而可能进一步增加移动支付市场的深度和广度。同时由于受到国内监管约束，其只定位为移动支付的硬件技术提供商，而非独立的支付账户生态体系，与现有监管的相容性也较好。与此相对应，具有我国特色的、拥有独立账户的第三方支付平台建设，未来的生态创新空间可能会越来越受到监管制约。

三是从国际视角来看，伴随人民币国际化和居民对外经济金融往来的飞速发展，更加便捷安全的跨境支付、海外支付将成为新的市场增长点，依托 APPLE 的国际布局优势，或许能够促进我国移动支付产业的边界拓宽、技术接轨前沿、卡组织与卡产品走向国际化等。

当然，也有一些产品内在的不足，使 APPLE PAY 也面临发展的约束。一方面是来自硬件环境的约束。众所周知，IPHONE 手机由于价格相对较高，且 Apple Pay 只能适用于 IPHONE6 以上的版本，因此其用户群体难以向广大中低收入人群拓展。同时，虽然银联在推动云闪付过程中，已经进行了大量 POS 终端改造，但这仍是 NFC 发展的重要制约，还需投入大量的成本推动 POS 端的覆盖面，这也使得 Apple Pay 的线下应用场景短期内难以有快速提升。同时，来自国内市场的零售支付“高频化”特点，也使得苹果的后台支持网络或许会常常面临“崩溃”的挑战，这在首发日已经有所体现。另一方面，从软环境的约束来看，Apple Pay 的线上支付同样更缺乏交易平台的场景支持。而在线下的发展中，国内用户除了便捷之外，已经习惯于支付巨头开展的补贴、优惠、红包大战，而这些似乎又不是习惯“高冷”形象的 APPLE

所想做的，因此短期内似乎也难以大幅提高其使用频率。

同时，就行业发展环境来说，在经历了首发的热炒之后，Apple Pay 仍需要拓展有效的业务模式。就短期来看，可能有来自第三方支付企业的产品竞争、HCE-NFC 的竞争、SE-NFC 模式下其他手机终端的挑战、非接触式卡支付、电信运营商的挑战等等，并且在经历了初期蜜月之后，银联与银行也需要使短期和长期合作利益逐渐落到实处。

就长期来看，一方面，在不同的发展背景与条件下，市场主体的“分分合合”也很正常，我们不用过于担心国内支付产业被 Apple 所“绑架”，低估国内市场主体的“智慧”。另一方面，更值得深思的是，以移动支付为代表的整个新型电子支付产业，最终可能从卡基向网基逐渐转换，过分依赖于硬件的“重”支付方式，必然逐渐过渡到各类“轻”支付模式。虽然这一过渡期可能仍然较长，传统支付模式在新技术引导下也仍可能有特定的繁荣周期，但如何面向未来可能的支付革命，是所有传统支付产业链参与者共同面临的挑战。

总的来看，Apple Pay 面临的机遇与挑战、优势与不足都比较明显，进入国内市场已经是其一个成功的重要举措。我们既不需要对其过于神话、夸大其给国内支付行业带来的正面或负面影响，也不能低估和漠视其给支付产业链带来的技术与商业模式冲击。应该说，技术进步和竞争充分，总是有利于一个行业的健康发展和消费者利益。在愈加精彩的移动支付大舞台上，Apple Pay 肯定是一个重要参与者，但究竟在支付变革大潮中掀起多大浪花，还有待历史检验。

第三方支付跨境业务的反洗钱风险及其防范

随着跨境网购市场的迅猛发展，第三方支付平台在跨境支付中的使用率大幅上升。第三方支付机构为网民跨境支付带来便捷的同时也为犯罪分子掩饰、隐瞒贪污贿赂、网络赌博、网络诈骗等犯罪所得开辟了跨境洗钱新通道，特别是近几年，越来越多的犯罪资金利用网络支付手段进行跨境清洗，第三方支付跨境业务的反洗钱风险愈发突出。

一、第三方支付跨境业务流程

通过第三方支付平台进行交易的类型有两种：一种是购买者（付款人）在境内，商家（收款人）在境外，如“海淘”；另一种是购买者（付款人）在境外，商家（收款人）在境内，即境外购买模式。本文主要分析境内不法分子如何利用第三方支付平台反洗钱风险漏洞向境外转移赃款，因此重点关注第一种交易类型。以支付宝进行“海淘”为例，其交易流程为：在境内的买家拍下境外商家的货品后，支付宝向境内合作银行查询汇率并向境内买家显示人民币交易价格，买家按显示的人民币价格支付相应款项到支付宝，支付宝向境外商家发出支付通知，境外商家向境内买家发货，同时，支付宝根据交易情况通过银行进行批量购汇，在买家收到货品后向银行发送清算指令，通过 SWIFT 直接将外币货款打入境外商户开户银行，完成交易。在整个交易过程中，客户身份、资金用途、交易性质隐蔽性强，交易背景复杂，交易持续时间长，洗钱行为难以被监测。

二、第三方支付跨境业务反洗钱面临的主要问题

（一）客户身份信息难识别

非面对面和跨国界的交易性质使得第三方支付平台难以有机会接触客户或账户的实际使用人。同时，由于不同国家和地区客户身份证明文件的多样性和跨境交易的复杂性，第三方支付平台尚缺乏身份识别的有效手段。一是客户身份信息的真实性难以核实。对境内客户，第三方支付平台目前尚未使用公安部联网核查公民身份信息系统，难以确保个人客户身份信息的真实性；对境外客户，第三方支付平台获取身份信息存在一定困难，即使客户提供了身份信息，审核人员也缺乏有效手段对诸如客户的职业、收入情况、通讯地址等信息进行核实。二是机构客户身份资料更新存在困难。第三方支付平台一般采用电话方式通知机构客户更新身份证明材料，但经常会遇到无法联系到客户或联系后客户迟迟不更新的情况。对于境内机构，第三方支付平台可以通过实地走访的方式进行联系提醒，但对于境外机构，尚缺乏有效手段与其再次取得联系，也缺乏核实其提供证件是否真实有效的途径。

（二）跨境交易真实性难审核

第三方支付平台由于获取境外客户的实际控制人、股权结构等信息存在困难， 难以判断客户财务状况、经营范围与资金交易情况是否相符，所以无法核实跨境交易金额和交易商品是否匹配，再加上对境外客户进行尽职调查的成本相对较高，造成审核工作流于形式。此外，第三方支付平台取得跨境支付业务资格的时间较短，相关配套制度不够完善，缺乏足够的审核经验，部分违法客户可能会利用这一漏

洞，制造虚假交易或虚假贸易合同向境外非法转移资金，为贪污受贿、出口骗税、黄赌毒等上游犯罪所得销赃。

（三）跨境可疑交易难监测

第三方支付平台通常是每天将所有客户当日所有交易汇总而非每笔交易明细发给收单银行，银行按照第三方支付平台的指令，将资金划入目标账户。第三方支付平台只能获取交易双方有限的交易信息，如订单号、银行账号等，而交易双方的姓名、职业等信息获取较难；银行的业务系统只能看到交易一方和第三方支付平台信息，无法查询交易对手的信息，因此一笔完整的交易（包括完善的客户身份信息和交易信息）被第三方支付平台和银行割裂，影响了双方反洗钱系统监测可疑交易的效果，增加了分析、甄别可疑交易的难度。以跨境网络赌博资金清算为例，境外的赌博公司在境内设立代理人，双方均以空壳公司名义在第三方支付平台注册成为客户，并虚构一笔商品或服务交易，境内代理人确认收到由境外赌博公司发送的虚假商品或服务后，第三方支付平台将境内代理人托管的资金转入境外指定关联银行账户。银行在跨境交易过程中，只负责核对支付机构名称和交易金额，并在交易附言中注明“跨境外汇互联网支付划转”字样，而无法了解交易双方的资金来源、资金用途、经营状况，也无法核实该笔跨境外汇业务的交易背景、交易用途、收付款人之间的资金来往关系。即使该交易被监测报告为可疑交易，监管部门在分析过程中，查询的交易记录显示交易双方为客户 A 和平台，而无法查看到客户 A 具体的交易对手客户 B，进而难以追踪、分析资金流向。

（四）互联网技术难支撑

目前，跨境支付业务迅速发展，互联网技术支持尚未完全跟上。一是反洗钱监测分析系统功能欠缺影响大额和可疑交易的分析甄别。第三方支付平台大额和可疑交易监测系统对于跨境支付存在参数设置不合理、模型设计不科学、监测范围和时间未能完全覆盖交易涉及区域内所有时段的全部交易等问题，影响提取大额和可疑交易的效果，容易造成漏报、错报大额和可疑交易报告。二是网络信息安全隐患可能引发客户信息和交易数据丢失风险。在大数据、云计算环境下，一些支付平台网络信息安全措施不完善，操作系统比较脆弱，易受到不同国家和地区黑客、病毒攻击；数据库系统的保密性、可靠性存在一定的安全问题，致使客户数据很容易被窃取或被篡改。

三、对策建议

（一）健全跨境支付业务反洗钱法规体系

一是在支付机构反洗钱法规规章中明确跨境支付业务的客户身份识别、客户身份资料和交易记录保存等操作细节。二是完善跨境支付业务反洗钱法律责任和处罚规定，加大对高风险支付机构的执法检查力度和处罚力度，督促支付机构优化资源配置，有效管理风险。三是明确支付机构和收单银行在信息传递中的反洗钱义务，便于监管部门事后通过收单银行加强对支付机构的监管，同时有效解决跨国境（地区）调查费时、费力和效率低的问题。

（二）完善客户身份识别措施

一是强化用户准入。在当地法律允许的情况下，引导个人用户进行实名注册，控制开户数量，强化机构客户实名制开户措施， 对非实名认证账户采取功能和额度等限制策略。二是采用多种识别方式。身份识别方面，在利用传统的 IP 地址、Mac 地址等终端数据进行识别的基础上，运用先进的生物识别技术，如指纹识别、人脸识别、掌纹识别、声波识别等辅助开展身份识别， 便于在持续识别和重新识别阶段进行比对判断；行为识别方面，通过客户的注册行为、浏览行为、购物行为等识别交易的风险，尝试使用较先进的技术辅助开展识别，如近期支付宝推荐的键盘击键识别；关系识别方面，通过各种社交网站如 Facebook、Twitter、LinkedIn 等引入数据，查寻客户之间的关联，将身份特征、关系特征和交易特征进行分类，提高识别能力。三是严格审核客户信息。对境外机构客户，采用多种渠道严格审核其资质、证照、经营范围等相关资料，如与境内、境外权威部门提供的公民或企业身份信息数据库进行比较核实，与行业间的共享客户信息资料中已有的客户信息进行比对，确保客户身份信息的真实性。

（三）严格审核交易的真实性

一是严格审核交易资料。对于货物贸易，要求商户提供物流凭证或信息；对于服务贸易，要求客户提供电子票号等信息，在此基础上进一步确认每笔交易的真实性，切实防范利用虚假交易进行洗钱的风险。二是通过共享合作机制核实交易信息。建立第三方支付平台之间风险共享与合作机制，防止犯罪分子在不同平台反复销赃； 加强与境内外银行合作，利用银行较成熟的风险防控成果核实客户身份信息

和账户信息；建立与其他企业合作机制，如邮递公司，核实客户交易信息的真实性。

（四）加强跨境交易资金监测和可疑交易分析研判

一是完善大额和可疑交易监测系统。建立健全风险识别体系，完善大额和可疑交易自动识别系统，设定相应的大额和可疑交易参数、模型，并定期进行维护、优化，确保大部分交易风险能够被识别。二是建立专业的分析团队。全球性交易对人工分析、甄别具有更大的挑战，分析人员不仅要掌握境内各地区的犯罪特点，还要了解不同国家和地区的经济、社会、人文、地理及犯罪特征等，培养高度的敏锐性，对交易信息进行全方位、多角度检索、分析，做出合理的判断，能够识别少部分未被系统监测的可疑交易。三是加大对敏感国家和地区的交易监测力度。对来自洗钱高风险或反洗钱、反恐怖融资监管薄弱国家和地区的客户采取强化的尽职调查措施，密切监测转入或转出这些国家和地区的资金交易，动态维护黑名单、灰名单数据库，认真核实客户是否属于名单监测范围，分析判断为可疑交易的严格执行可疑交易报告制度。

（五）加大网络科技投入

一是完善识别、监测、查询系统功能。根据业务发展情况，不断完善客户身份识别、大额和可疑交易监测、客户信息和交易记录查询系统的功能，以支持先进的生物识别方式、监测新型洗钱类型、回溯已完成的交易记录等业务。二是提高安全、保密技术水平。不断研发、更新智能防火墙、加密、反病毒等网络信息安全技术，加强管理，防

止缺损、泄露客户信息和交易数据，建立回溯性分析机制，确保已支付的交易能够完整、真实、及时重现。

厘清数字货币的内涵与挑战

近期，央行召开数字货币研讨会，周小川行长也就此接受了采访。这一公众相对还较陌生的概念，迅速引起了各界的关注和热议。实际上，虽然近年来数字货币已经成为业内流行的全新概念，但迄今为止，还没有统一的内涵边界。

如果要追根溯源，则需从电子货币的概念着手讨论。根据巴塞尔银行监管委员会（BCBS）的定义，电子货币是指通过销售终端、设备直接转账或电脑网络来完成支付的储存价值或预先支付机制。国际清算银行（BIS）早在 1996 年就开展了一系列研究，并认为电子货币可能会影响到中央银行的货币政策，如影响央行控制的利率和主要市场利率的联系。

客观来看，一方面，长期以来央行依然具有垄断性的货币发行权，同时也基本掌控着主要电子货币的发行权。另一方面电子货币也给货币政策理论框架带来很大冲击，因为“货币”的可控性、可测性、相关性都在发生变化。当然，随着新技术日新月异的变化，逐渐出现了可能脱离央行控制的新兴网络电子货币形态。在新技术的冲击下，究竟什么是“货币”可能越来越说不清楚了，其概念、范畴、转移机制都在发生变化。其中，大额与小额、银行与非银行、中心与去中心，引起了不同形态的货币及货币转移带来的深刻影响，这体现为对货币数量、价格、货币流通速度、货币乘数，以及存款准备金等制度的冲击。

进一步梳理电子货币的发展脉络，需要从货币背后的信用最终支撑入手。

其一，最为典型的法定电子货币的信用支撑，或者直接来源于各国央行，或者是由银行业机构提供直接支持，央行依托委托——代理关系给予间接信用支撑。以信用卡为代表的传统电子支付创新，以及金融机构电子钱包的出现，实际上都属于货币的形态和体现发生了变化，但没有跳出央行信用直接或间接的覆盖范畴。

其二，伴随着电子商务的发展，越来越多的非银行机构介入电子支付工具的提供之中，也对货币结构和范畴带来新的影响，其信用最终性支撑与央行的联系变得更弱一些，因此成为各国监管的重点。如欧盟专门制定规则，用以规范在信用机构之外发行以电子货币为支付方式的企业或任何法人。

其三，在多元化的网络经济时代，也出现了由某些“网络货币发行主体”提供信用支持的虚拟货币。如果这些虚拟货币最终用于购买程序开发商所提供的电子产品，则交易中真正发挥媒介作用的是现实中的货币，虚拟货币并未形成独立的电子货币。如果虚拟货币不是从程序开发商中兑换获得、且交易对手不是货币发行方（程序开发商），那么这种虚拟货币就可能独立地在虚拟世界里执行其商品媒介的功能，如游戏玩家间在淘宝网上用人民币交易某种游戏币。当然由于规模通常较小，其对现实经济的影响并不显著。

其四，上世纪 80 年代，一批国外专家开始研究基于特定密码学的网络支付体系，并且探讨了匿名密码货币，由此出现了作为电子货

币高级阶段的、新型数字货币的萌芽。到2008年日裔美国人中本聪发表论文描述比特币电子现金系统，2009年比特币诞生，使得数字货币探索到了新阶段。当然，目前数字货币多少都存在各种缺陷，比特币的资本属性也似乎多于货币属性，并且常常陷入炒作带来的价格波动中。

总的来看，严格意义上的数字货币属于最后一种，更多开始依托分布式规则、智能代码来发行和运行，其信用支撑已经距离央行的中心化机制越来越远，虽现在规模尚小且技术还需成熟，但未来对现有货币机制可能带来重大影响。至于区块链技术则属另一层面的概念，例如当我们谈到比特币时，它实际由区块链底层技术（协议与客户端）和现实存在的加密数字货币组成。依托于区块链或其改良技术，也出现了其他一些类似比特币的虚拟货币。此外，虽然是当前最典型的技术，但数字货币的底层支撑不一定限于区块链，同时区块链也可以进一步拓展到货币之外的各类去中心化价值交换活动。

因此，当我们谈到数字货币的时候，一种强调的是新型的电子货币，可以利用加密技术实现独立于中央银行之外，按照特定协议发行和验证支付有效性；另一种则是对现有电子货币典型模式的进一步优化，从而既引入包括赋予货币智能代码之类的新技术支持，又保持央行对货币运行的适度控制力。就我国央行来看，短期内应该更为关注的是后者。

实际上，这一挑战也是全球性的。例如，美联储在2015年初发布的《提升美国支付体系战略》中指出，“与通过中心辐射状网络结

构清算交易相比，金融机构间基于公共 IP 网络的信息分布式架构有可能降低成本。中央当局要在中央总账里建立报文标准、通信、安全和记录交易的通用协议，以便利相应的银行间结算”，这与改良型的数字货币创新事实上是一致的。美联储还提到“分散式数字价值转移工具目前还未成为足够成熟的技术，但是考虑到市场对此的强烈兴趣，这种方案将进一步研究并监测”，后者则更类似于真正去中心的数字货币。

从现金到非现金支付、从传统卡基电子支付到网基电子支付、从简单电子形态支付到智能代码支付、从支付工具层面到货币层面，应该说新技术在不断改变着货币金融体系。最终有可能带来更高的交易效率、更低的成本、更精准的政策执行、更有效的反洗钱等风险控制等，从而深刻改变着老百姓的生活，并使我们有可能在全球货币体系变革中争取更多话语权。当然，这些目标并非轻易能实现，夸大或低估其影响都是不理性的，还需大量的研究探索，专业的普及与公众教育，从而“挤出”数字货币领域的违法者、投机者与行业“劣币”。

无现金社会离我们多远

近期，据彭博新闻社称，欧央行理事会已同意成立小组，研究废除500欧元面值纸币的技术细节，旨在打击犯罪活动。众所周知，各国大额纸币发行除了与通货膨胀有关，还有其他因素。如最初500欧元面值主要是尊重个别国家使用大面额钞票的传统，也可免除跨国刷卡的服务费。但在现实中，虽然大额或小额纸币都可能被用于非法活动，但也不应高估纸币的影响。例如，据联合国毒品控制和犯罪预防办公室发布的《2011世界毒品报告》，全球每年毒品交易额达8000亿至1万亿美元，绝大部分是通过银行进行洗钱。同样在我国，据央行发布的数据，仅2015年4月至11月，就破获地下钱庄转移赃款案件92起，涉案金额8000多亿元。这些典型的洗钱犯罪，显然是与纸币无关，而是现代金融体系的“灰色产物”。

然而，现金使用比率的下降，确是不争的事实。其根源还是电子支付、电子货币带来了更高的效率和更低的成本，当然也有助于“魔高一尺、道高一丈”的违法追踪与风险控制。根据可得最新数据，凯捷(Capgemini)与苏格兰皇家银行集团（RBS）联合发布的《2015年全球支付报告》显示,2014年非现金支付交易量增速预计达到8.9%，高于2013年的7.6%，创下3897亿的交易量新高。另据国际清算银行(BIS)统计，2014年19个最大经济体的流通中现金余额为国内生产总值(GDP)的7.9%，2010年则为8.4%。

目前，我国的非现金支付增速也已居全球前列，近年来银行和非

银行支付机构的电子支付业务较快增长，其中，由于网络经济的快速增长、智能手机用户数量的大幅提升，使得我国成为全球范围的移动支付高增长区域，也是新支付技术的实践“热土”。

无论在发展中国家还是发达国家，新兴电子支付不仅能够替代纸币的支付功能，而且能够依托支付渠道解决弱势人群的金融需求。例如，肯尼亚 M—Pesa 手机银行的出现，使得移动业务与家庭汇款等基本金融需求密切结合起来，充分体现了移动支付的高效率和低成本，较好地解决了落后地区的支付需求。再比如，美联储在 2012 年发布的报告就表明，在美国的消费者中还有大约 11%的人无法享受到银行服务，另有 11%的人只享受较低水平的银行服务，而与充分享有银行服务的人相比，这些人往往属于弱势群体，但他们却多数都拥有智能手机，并且更愿意使用移动银行和移动支付。由此来看，在我国，除了城市的中低收入人群，广大农村领域也应是以新兴电子支付来践行普惠金融的重要试验田。

在政策支持和科技进步驱动下，似乎全球都不可避免从现金走向电子支付。2013 年挪威学者 Trond Andresen 曾在一篇工作报告中指出，“实物货币的必然消亡只是个时间问题”。当然，这一过程可能仍然是漫长的，因为纸币仍然有其需求空间。例如据统计在美国，50 到 100 美元间的交易只有 16%用现金，而 1 美元以下的交易则有 66%以现金完成。由此来看，无现金社会也需要支付习惯的转变，以及电子支付真正在低成本、便利与安全之间做到极致。

从公有链到私有链：区块链回归现实

应该承认，比特币区块链当初是一群极端无政府主义者创造出来的，他们试图在虚拟世界里过无约束的生活。但是，当比特币创业公司开始接受风险投资，董事会里的资本方代表，必然要求那些公司到现实世界里去实现股东的价值。为此，过去几年，我们看到了比特币公司创始团队分裂和董事会里传统金融机构人员增加的现象时有发生。

从 2009 年 1 月开始运行的比特币区块链，至今已经有七年时间了。即使是最保守的观察者都注意到：这个基于分布式网络的点对点数字货币交换系统，在无中心服务器，无运维管理的情况下，没有出现过一次宕机，而任何中心机构的数据中心都做不到这一点；这个价值交换系统每周七天，每天二十四小时运作，实时结算，实时到帐，交易费用几乎可以忽略不计。

作为冷眼旁观者的传统金融机构，在长期观察比特币这个实验之后，不再无动于衷。他们看到了区块链技术的这些优势，感觉到这项技术改造传统金融系统的前景和价值。于是，从 2015 年开始，欧美的主流金融机构纷纷设立自己的区块链创新实验室，探讨在各种金融场景中，应用区块链技术的可能性。

渐渐的，他们发现：区块链技术将会给金融行业带来一场革命！区块链技术（Blockchain）是互联网世界里的一个应用协议（价值传输协议），它和 HTTP（文本传输协议）协议一起，构成了互联网发展

历史上最重要的两个应用协议。文本传输协议解决了互联网点对点信息传输的问题，把互联网带入到信息互联网阶段；价值传输协议解决了互联网点对点价值传输的问题，把互联网带入到价值互联网新阶段。

区块链技术将从基础网络开始，重构传统金融业的底层架构，让传统金融业有机会用价值互联网技术把自己改造为互联网公司，把所有的金融服务场景都互联网化。从而拥有与支付宝和微信支付等互联网金融企业一样的技术基础。互联网金融与传统金融的一个基本的区别在于网络架构：后者是基于电路网络，通过程控交换机来进行数据交换，交换需要两端建立直接联系（像打电话那样，对方得有人接）；前者是基于 IP 网络，通过网络路由器来进行分组交换，交换不需双方建立即时直接联系。支付宝和微信支付就是基于 IP 网络的金融服务，而传统金融业还是基于电路网络的金融服务。IP 网络可以传输非结构化数据，比如音频，视频，图片，而电路网络只能传输音频和数字。IP 网络可以做到随时随地的，随心随愿的服务，因为它不需要建立即时直接联系。区块链就是一门用来帮助传统金融业在 IP 网络上重建基础设施的互联网技术。

观察到这一点，也就难怪欧美主流金融机构纷纷开始实验区块链技术，来改造自身的业务流程了。但在实验区块链技术的过程中，鉴于现实世界的法律合规的要求，尤其是政府对于持牌金融机构的了解你的客户（KYC）及反洗钱（AML）方面的严格要求，比特币那样的透明、共享的公有区块链不能完全满足持牌金融机构或者其他一些中心

化机构的合规要求。于是，现实需求催促区块链技术的发展，私有区块链应运而生。

在过去一年多时间里，区块链社区对私有区块链存在的价值和意义，有一些争论。最主要的争论在于：私有区块链可能与中心化数据库没有区别，属于画蛇添足。我非常同意万向区块链实验室首席科学家、以太坊智能合约（世界上最主要的两个公有区块链之一，另一个是比特币区块链）创始人 Vitalik Buterin 的观点：私有区块链的优势有五点：一是交易的效率更高。比特币区块链目前每秒可完成七笔交易，而私有链目前可以最高到每秒十万笔，并且还有提高的空间。这显然更适应现实世界金融交易的需求；二是交易可以回滚。这点对于中心化机构也很重要，在某些情况下，某些交易会因为错误或法律的问题而被要求修改、撤销；三是交易费用更低。目前公有链的交易费用是每笔 0.01 美元，而私有链的交易费用将会降低一到两个数量级；四是仍然是基于分布式网络，保留了分布式记账系统的优点。五是私有链提供了更好的隐私保护。公有区块链因为其透明共享总账本的设计，本身不提供隐私保护功能。比特币账户的私钥好比户名，公钥好比账号，矿工挖矿就是解码公钥，因此账户是透明的。这显然不符合现有法律框架下的金融机构的要求。于是技术再一次跟上了现实世界的需求，人们开发了多重签名技术及零知识证明技术，来在私有链上进行符合现行银行保密法规的隐私保护。零知识证明技术使得人们可以在不需共享账户信息的前提下，基于区块链的分布式记账系统仍然可以有效的运作。

很显然，区块链社区对私有链的分歧，并不在于技术路线层面，而是在于价值观层面。对区块链技术最初的去中心化功能的向往，使得一些人故意忽略了私有链在对接现实世界需求上的价值。其实，只要能够造福人类社会，为什么要那么绝对的支持一方，拒绝另一方呢？公有链自有共有链不可忽略的价值，自有它独特的应用场景。我认为，区块链的去中心化并不是反中心化，它只是人们基于降低成本和提高效率的千年不变的商业原理，利用区块链这个新的技术，去掉那些已经蜕变为高成本、低效率的中心。根据对全球区块链实验项目的观察，我们看到的大部分事实是，区块链实际上只是帮助做到了多中心、分中心，或者是在区块链技术的基础上创建了新中心，一个能够提供更低成本、更高效率的新中心。区块链作为互联网点对点价值传输技术协议，我们还是要秉持技术中立的基本立场，客观看待公有链、私有链各自的特点和优势，在能发挥各自优势的地方，让它们各自挥舞各自的大旗吧！

在公有链、私有链之外，还有一种由几个中心化机构联合发起的，介于公有链和私有链之间的，兼具部分去中心化功能同时分布式网络节点又受到控制的区块链，人们把它命名为联盟链。在联盟链中，每个区块的交易确认，都需要联盟各方的大部分成员来达成共识。最近，美国的银行区块链联盟组织 R3 就宣布，它的四十二个会员中的十一个银行，已经在微软的区块链云平台上，基于以太坊区块链，实验运行十一家银行的联盟链。联盟链就是传统金融机构作为中心化机构，希望兼顾分布式网络的健壮、去中心化账本的优点、高效率的交易确

认速度、可控制的网络节点、可靠的隐私保护等公有链和私有链的好处的一个尝试。

这个实验非常值得期待。如果实验取得预期的良好进展，那么前几天中国人民银行发布的，关于中国要研究发行数字货币的可能性的消息，其中的一个最大的技术难题：基于哪种区块链技术平台，采用哪种区块链运行模式的问题也就有了参考答案。我认为，中国人民银行如果要发行自己的数字货币，只能在自己建立的联盟链上来发行。所有参与银行的数据中心构成这个联盟链的分布式网络，从而保证这个联盟链网络的健壮，永远不会宕机；得到中国人民银行认可的国内外金融机构，可以成为网络节点，参与共识记账；采用零知识证明技术，确保各个参与者的信息不会泄露；各个银行的中心数据库作为核心节点，完整复制全账本，其他认可接入机构作为二级节点，只记录账本的索引，确保达到高效与高可靠性的结合。这将非常有助于人民币有序、可控的国际化。中国央行通过认可全球金融机构接入中国央行的联盟链，利用了区块链数据库的数据透明共享、不可更改、不可撤销、可追踪、可编程的特点，对国际市场人民币的流动踪迹可以做到一目了然，心中有数。而且，也可以省去纸质人民币印刷和运输的成本。更重要的价值在于：通过建立这个联盟链，根据区块链技术信息流与资金流合二为一、每十分钟结算一次、净额交收改为实时逐笔交收、系统每周七天，每天二十四小时运转的特点，事实上也就建立了一个目前最高效的全球化的人民币登记结算、支付清算网络。这个

崭新的人民币的登记结算、支付清算网络的管理控制权将完全掌握在中国人民银行的手中。

综上所述，建基于虚拟世界，起源于数字货币，力图去中心化结构的区块链技术，在过去近两年的时间里，由于内外的种种原因，逐渐的向现实世界回归，开始在连接虚拟世界与现实世界的过程中，展现出它更广的前景、更大的价值。由此也吸引了传统金融机构对它的兴趣，引来了数以十亿美元记的风险投资。这又反过来极大的促进了区块链技术的快速发展，使得区块链社区由草根阶层摇身变为高大上阶层。尤其在最近的几个月时间，我们可以明显的感觉到，区块链技术几乎要进入指数级增长阶段，每个月都有新的技术在发展中。这迫使我们万向区块链实验室修改了全球区块链开源软件赞助计划，从原计划的每半年一次，修改为每两个月一次，以因应全球区块链技术的发展趋势。在区块链技术迅速与现实世界接轨的过程中，在传统金融机构的热切介入之下，我认为区块链技术已经进入了它自己的"摩尔定律"发展轨道。信息互联网从上世纪九十年代初期发轫，到今天发展了二十多年，对人类社会的影响可谓天翻地覆。我大胆的预测，价值互联网对人类社会的影响进程，将大大加速，从今天开始就将进入指数级增长阶段！

（作者：肖风　万向区块链实验室发起人、中国区块链研究联盟副主任）

区块链冲击全球金融业

信任是金融业的基础！

我们相信中央银行的兑付允诺，所以我们使用央行发行的法币进行交易；我们相信托管人的信誉，所以在证券市场中我们将资产交由其保管；我们相信复式记账法和注册会计师的信誉，所以我们使用经审计的财务报表进行投资决策；甚至，在网上购物时，我们相信“淘宝”等第三方的支付承诺和信用承诺，所以我们将货款交予其支付。为了维护信任，金融业的发展催生了大量的中介机构（包括托管机构，第三方支付平台，公证人，银行），然而由于中介机构处理信息依赖人工，且交易信息往往需要经过多道中介的传递，这使得信息出错率高，且效率低下；同时，人们通常认为权威机构公示的信息是经过社会认可的信息，不存在欺诈风险。实践中，权威机构通过中心化的数据传输系统收集各种信息，并保存在中心服务器中，然后集中向社会公布。这种中心化的传输模式同样使数据传输效率低，成本高。

如何高效，便捷，且低成本地建立信任，成为为业界关心的问题。区块链通过数据的分布式存储和点对点传输，打破了中心化和中介化的数据传输模式，满足业界的需求。这无疑将对金融业产生深远影响。

美国《华盛顿邮报》网站 2016 年 1 月 6 日刊文指出，区块链是 2016 年最有可能改变创新之路的十大最前卫的创技术，区块链或许是互联网出现以来的最重大发明。全球知名大金融机构如高盛、美洲银行、UBS 等 42 家银行都加入了一个名为“R3”的组织，共同开展

对区块链的研究；德勤 DC3（德勤加密货币社区）也于 2016 年新年伊始在 Coin Desk 网站上发表了文章，基于对欧美商业社区的调查，我们预言区块链将在 2016 年走出实验室，变为现实。

那么我们这里就需要讨论如下内容。

一、什么是区块链？

提起区块链，很多人可能会感到非常陌生。然而当提到比特币，则大家对此可能已经耳熟能详。没错，区块链就是支持比特币的核心技术。比特币的概念最早由一位自称“中本聪”的加密专家于 2008 年提出，比特币随后应运而生。由于各种包括政府政策在内的内外在因素影响，比特币在近些年呈现大起大落的态势，前景不甚明朗。然而其核心技术，即区块链，则越来越受到全球金融业的关注。

区块链可以被理解为一个基于计算机程序的公开的总账，它可以记录在区块链上发生的所有交易。区块链中的每个节点都可以将其记录的数据更新至网络，每个参与维护的节点都能复制获得一份完整数据库的拷贝，这就构成了一个去中心化的分布式数据库。这种分布式的数据库可以在无需第三方的介入的情况下，实现人与人之间点对点式的交易和互动。同时，数据一旦被写入区块就不能被撤销，在 10 分钟内该区块中的信息将会被拷贝至网络中的所有区块，这就实现了全网数据的同步。区块链建立在互联网的基础上，任何接入互联网的端口都可以接入区块链。

二、区块链有哪些特征？

区块链具有可靠性和可用性的特征。区块链的设计使它能够有效预防故障与攻击。一个区块链通常是由一个开放的用户群所共享，整个区块链网络中单一节点出现故障，并不会导致其他节点上信息的缺失，其余参加者仍能照常运行，区块链上进行的金融交易不会由于传输问题受到干扰。

区块链具有透明性的特征。具体来说，任何数据的更新都会被同步至整个区块链上，区块链网络上的任何节点都可以查询整个区块链上的数据记录。这提高了网络上数据的可审计性，审计师可以实现对网络中数据的全范围审计。同时，区块链使用者能够实时获得区块链中全部数据，消除了信息不对称造成的风险，这提高了用户对网络中信息的信任度。汇丰银行分析师 Anton Tonev 和 Davy Jose 表示，区块链针对“如何在分散的系统中验证信任”这一问题提供了最优方案，这项技术最大的突破即陌生的两个人不再需要一个共同信任的第三人实现相互信任。

区块链上储存的记录具有不可改变性的特征。这降低了交易中的欺诈风险。而且储存的记录具有不可撤销的特征。当新数据写入区块后，新生成的区块将会被拷贝至区块链中的全部区块，这样的流程不可逆转，因此区块链具有不可撤销性的特征。这提高了交易的精度，也简化了数据处理的流程，更降低了保持数据原始性和交易可追溯性的成本。

区块链具有数字化的特征。由于几乎所有的文件或资产都能够以代码或分类账形式体现，这意味着，这些数据都可以被上传至区块链。

通过对区块链上的数据处理程序进行设置，智能合约及自动交易就可能区块链上实现。加拿大籍编程天才 Vitalik Buterin 创建的“Ethereum”系统即实现了这种可能。区块链的这种特征决定了其应用前景将非常广泛。

三、区块链和其他信息技术有何异同?

当谈及区块链时很多人会问，它与其他技术，比如互联网，社交网络，及传统数据库相比，有什么差别？ 下面的表格简要列举了其中差异：

	区块链	互联网	社交网络	传统数据库
主要用途	储存信息/记录交易	发送和接收信息	沟通交流	储存信息
去中心化	是	是	否	否
高度防篡改	是	在某些情形下	否	否
在线	是	是	是	否
适合私人使用	私有区块链适合在同一个组织的多方使用	是（内联网）	否	是

(一)区块链 v.s.互联网

区块链基于互联网来运行，但其功能广于互联网。两种技术的相同点主要在于：在数据传输方式上，互联网与区块链都不需要中心化的中介；两种技术都要求用户接入互联网；两种技术都能够满足一个组织内的多个使用者同时使用。两者的差异点主要在于：互联网技术的主要用途是实现信息的快速发送和接收，而区块链的主要用途则是实现数据的储存和记录；区块链上的数据具有高度防篡改性，而互联网数据只有在实现加密等保护性措施的前提下，才具有防篡改的性能。

(二)区块链 v.s.社交网络

社交网络是指类似于 Facebook 的网络沟通平台，它与区块链一样需要基于互联网运行，但却有明显的不同：社交网络的主要用途是为人们沟通交流提供一个平台，而区块链除了实现信息的共享外，还具有储存信息的功能；社交网络需要用户将信息发布至一个中心服务器上以实现共享，而区块链上的共享不需要一个中心化的服务器，使用者直接通过 P2P 的方式沟通；社交网络上信息的防篡改性很差，而区块链中的信息具有很强的防篡改性；社交网络的作用在于拓展人们现实生活中的社交圈，使用人数越多，社交网络越具有活力，这决定了它不适合私人小圈子使用；而区块链却可以适应小型组织中的信息共享。

(三)区块链 v.s.传统数据库

传统数据库和区块链都有数据存储的功能，然而区块链的性能远超数据库：传统数据库需要建立在一个中心服务器上，而区块链的分布式存储机制使网络中每个节点都拥有整个网络的数据；传统数据库由于保存在一个中央服务器上，数据被篡改的风险非常大，然而在区块链中，分布式的存储和透明化的查询使数据被篡改的可能性大大降低；传统数据库可以被离线保存在一个服务器上，而区块链要求所有节点必须接入网络，这种在线保存的方式保证了数据的时效性。

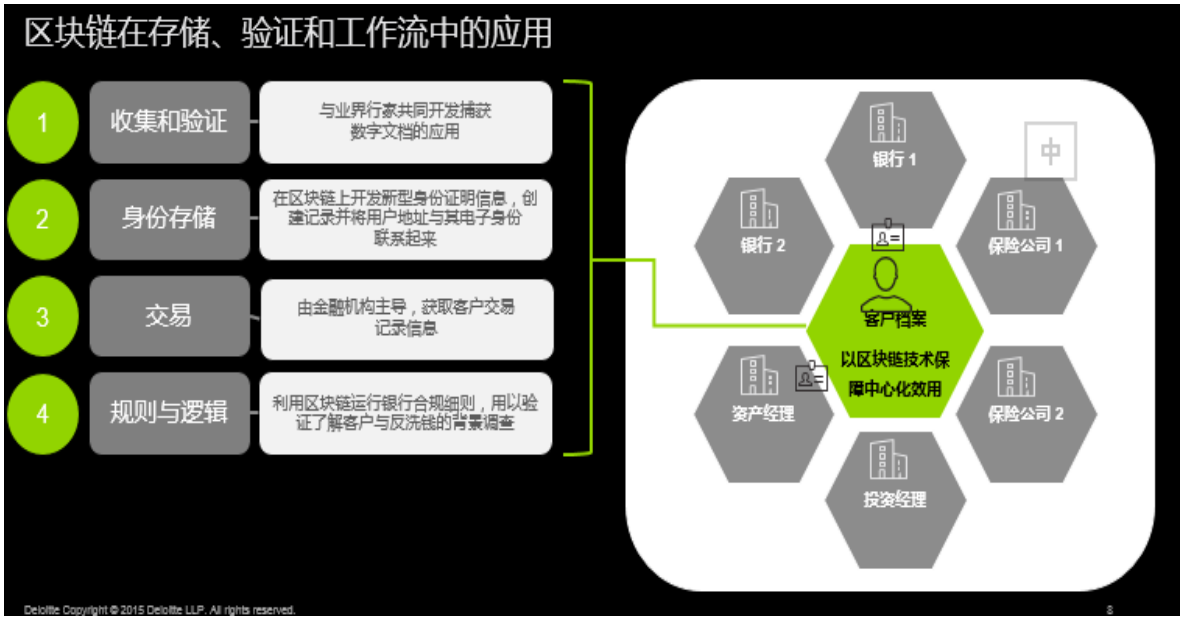
四、区块链将怎样应用于金融业?

区块链在金融服务业上运用最早也是最普及的场景包括支付，证券的清算和交割。DC3(德勤加密货币社区)在过去两年与全球商界的

沟通和讨论后，已经开发的区块链应用达到 50 多个应用案例，遍布金融，汽车，酒店，连锁业，医疗生命，媒体娱乐等行业。下面我们选取介绍德勤近期针对托管行领域完成的 4 个应用案例：

(一)区块链应用于金融机构的反洗钱（AML），了解客户（KYC）领域；

德勤应用区块链在反洗钱（AML）和了解客户（KYC）上颠覆金融业现存的合规模式。



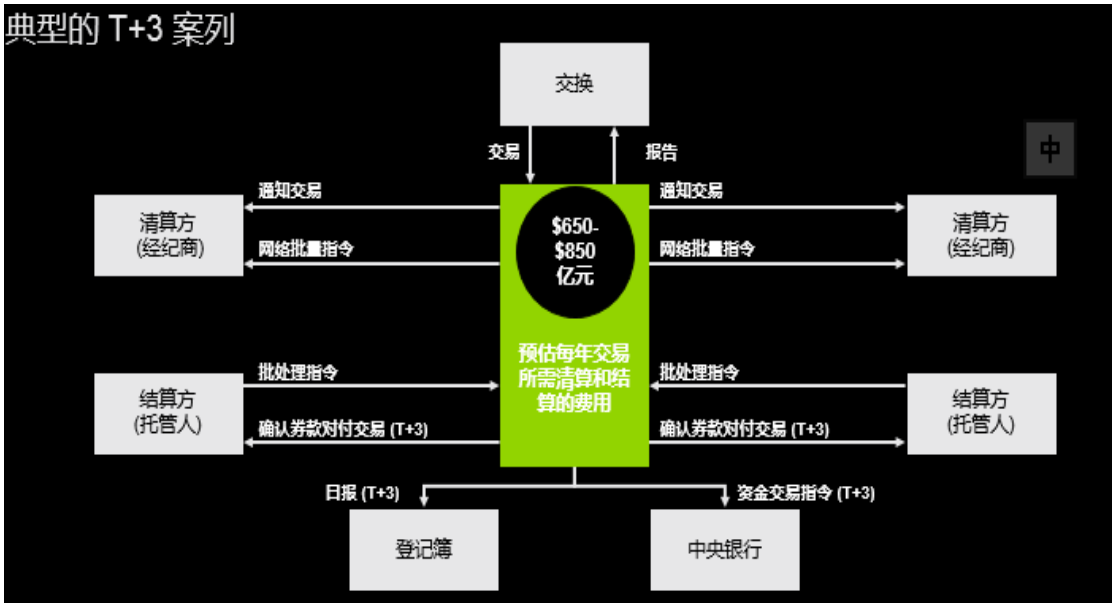
在反洗钱（AML）领域，基于区块链，各金融机构将各自收集和验证的客户信息数字化后，上传至区块链；同时，金融机构为交易中的实体提供电子身份证明信息（类似私钥），并将用户地址与其电子身份证明信息联系起来，任何交易的发生都需要经过该私钥和银行手中的公钥验证，并由用户地址进行，这就决定了区块链上数据的可追溯性。在这种模式下，各个金融机构在区块链上实现交易信息的共享，任一交易的任一环节都不会脱离监管的视线，黑钱将无处无法洗白，

这将极大地增强反洗钱的力度。同时，通过在区块链上设置的一定的规则与逻辑，区块链将自动验证交易和用户的合规性，不合规的交易及用户将被去除，整个金融企业的合规程度将得到提高。

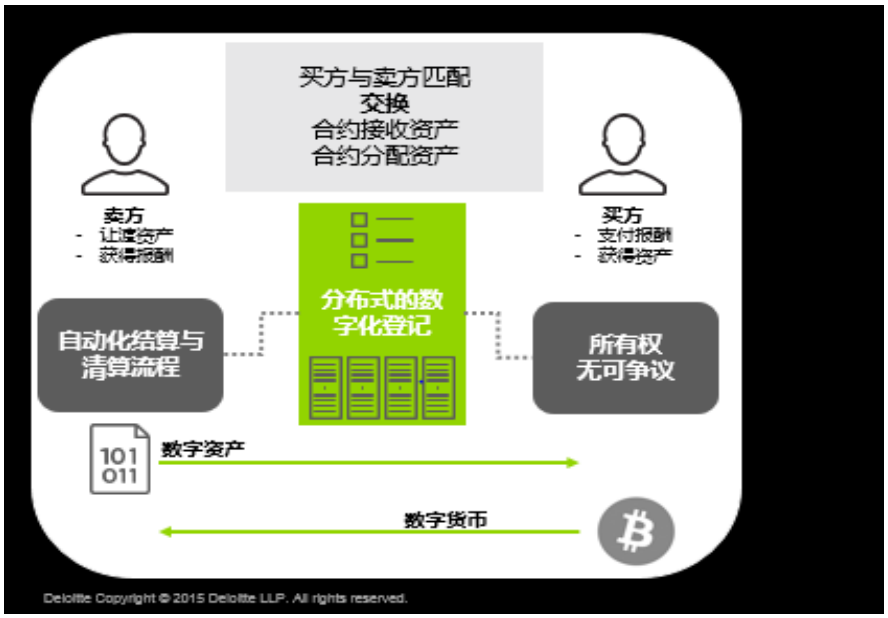
在了解客户（KYC）领域，金融机构同样可以通过区块链共享交易实体的信息，这将减少大量重复性工作，也为各家机构节省大量合规成本。同时，这将为金融机构在挖掘潜在业务机会，识别风险暴露方面提供很大帮助。

(二)区块链在证券结算和清算领域的应用。

证券结算和清算系统中典型的“T+3”案例：



区块链应用于证券结算和清算系统：



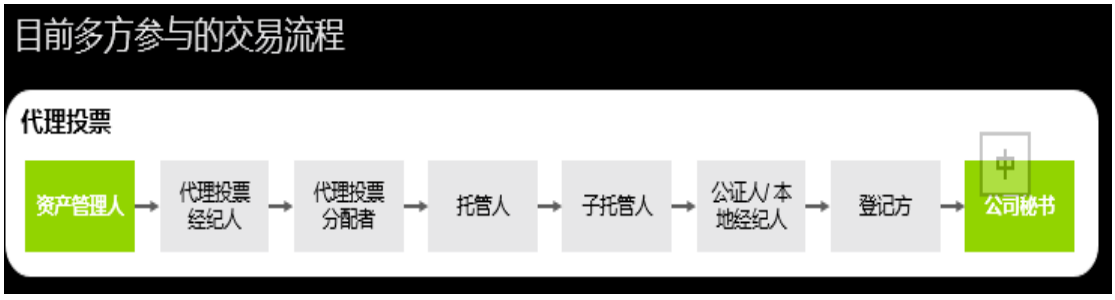
证券交易市场是区块链存在潜在发展机会的领域。在传统证券交易中，证券所有人发出交易指令后，指令需要依次经过证券经纪人，资产托管人、中央银行和中央登记机构这四大机构的协调，才能完成交易。整个流程效率低，成本高，且这样的模式造就了强势中介，金融消费者的权利往往得不到保障。一般地，从证券所有人处发出交易指令，到交易最终在登记机构得到确认，通常需要“T+3”天。有估算，美国两大证券交易所每年所需清算和结算的费用预估高达650-850 亿元，但如果将“T+3”天缩短一天为“T+2”，每年费用将减少 27 亿美元。

使用区块链，买方和卖方直接通过智能合约实现自动配对，并通过分布式的数字化登记系统，自动实现结算和清算。由于录入区块的数据不可撤销且能在短时间内被拷贝到每个数据块中，录入到区块链上的信息实际上产生了公示的效果，因此交易的发生和所有权的确认

不会有任何争议。与以往交易确认需要“T+3”天不同，在区块链上，结算和清算的完成仅仅需要 10 分钟（即在区块链上确认完成一笔交易的时间）。NASDAQ 的 LINQ 为 Overstock.com 在 2015 年年底发行的私募债就成功实线了这个场景。去中介化的交易流程毫无疑问将大幅度节省交易费用。

实践上，澳洲证券交易所（ASX）正在认真考虑将区块链应用于其清算和结算系统。据悉，纳斯达克 OMX 以及伦敦证券交易所，都已在探索这方面的应用。

(三)区块链在代理投票领域的应用

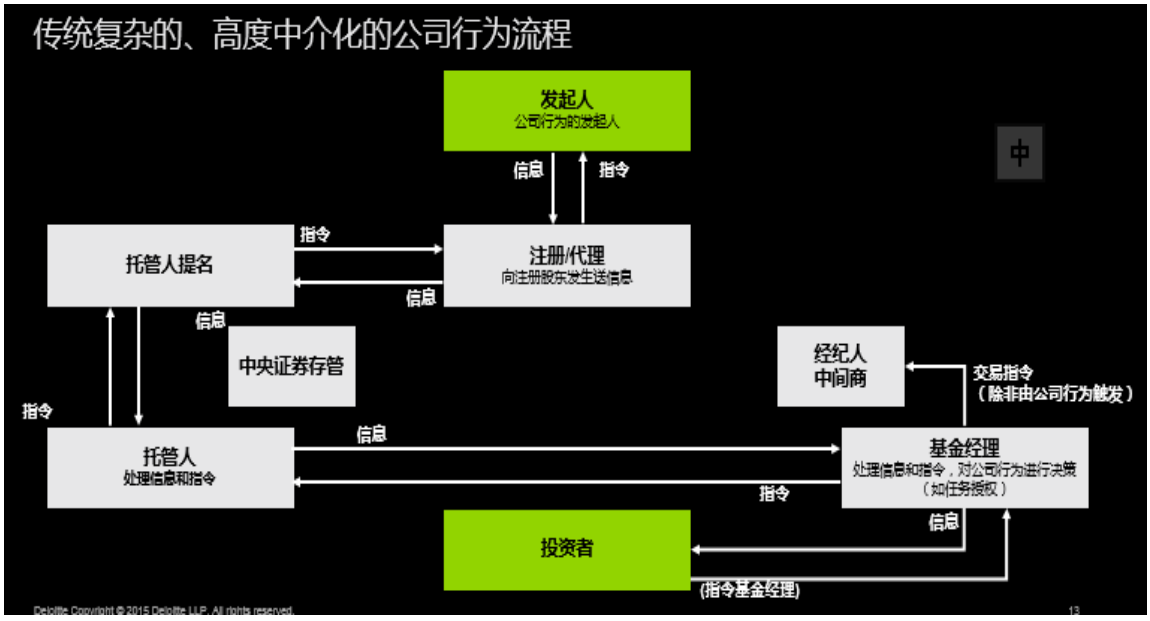


目前广泛运用的股东代理投票机制是由一套繁杂的程序构成的。通常资产管理人向代理投票经纪人发出投票指令，指令随后被传递给投票分配者，再由投票分配者将指令传递给托管人以及子托管人。托管人请求公证人对投票指令进行公证，然后向登记方申请并完成登记，最后投票信息汇总到公司秘书那里。这是一个非常复杂且非标准化的

流程，投票信息存在被不正确传递或丢失的风险。此外，由于托管人及子托管人使用不同的传输系统和字符识别系统，这导致投票的追溯和确认非常困难。荷兰一家研究机构就代理投票进行了研究，研究成果指出，在荷兰使用代理投票系统的公司中，仅仅有 31%的公司能够确认自己代理投票的结果。

例如，德勤使用区块链改变这一流水线型的流程。资产管理人只需下载投票软件，提交身份信息并完成注册，即可直接提交投票。投票结果一旦被成功提交至分布式数字化的投票登记系统后将不能再被撤销，同时由于区块链上数据的同步性，资产管理人可以很快地查询到投票结果。这一投票流程将较传统模式将节省 50%到 60%的成本，且同时具有安全，透明，高效，便捷的属性。纳斯达克 CEO Bob Greifeld 表示，纳斯达克将很快上线区块链代理投票应用，人们从此将能够在手机上投票并永久享有投票记录。

(四)区块链在公司行为领域的应用



与上文提到的证券清算结算和代理投票一样，公司行为领域的业务流程同样是高度中介化的。一项指令从公司投资人传递到公司行为的发起人，需要经过基金经理（经纪人），托管人，代理人等多道程序。复杂且高度中介化的流程使公司行为决策流程冗繁而昂贵，并往往会导致欠佳的交易决策，例如，权益的错误计算及选举的失败。

例如，德勤开发的区块链运用场景，在这一领域也取得了突破。和使用区块链的应用程序一样，这种新型公司行为管理系统免去高度中介化的流程，能够使投资人直接参与公司行为的管理，具有安全，透明，便捷，高效的特点。据悉，区块链公司 Symbiont 正在建立第一个基于区块链的智能证券交易与发行平台，该平台可以实现自动化的公司行为管理，该平台的投资人包括 NYSE Euronext 的前 CEO Duncan Niederauer。近期，德勤也将发布白皮书，区块链改变全球资产服务行业。

五、区块链的展望

区块链是一项很年轻的技术，它的运用和本身功能的继续开发在不断地进步和完善中。

区块链的进步和成熟需要工程师们的不懈努力，也需要商界领袖，专业服务机构和监管当局的共同支持。作为一个创新技术，当务之急是需要有志之士不断探索其应用的场景并根据商业需求，对工程师们提出技术上的开发要求。在运用场景尚未完全定义的市场里，我们不必纠结急于对区块链这个称谓的定义，而是要普及区块链本身的特征

和追踪它的发展变化，让商业机构甚至公共部门都利用技术带来的红利。

国内这方面的实践也在快速推进，2015 年 10 月，万向区块链实验室召开了首届全球区块链峰会后。此后，德勤和万向区块链实验室在 2016 年新年伊始，举办了首届上海区块链黑客马拉松，在 48 个小时的编程中，来自全球的近 100 位工程师创建了 23 个商业运用的模型，从医疗到食品，到进出口运输，到 REITS 的发行，其中绝大部分都很强的商业运用可行性。如果把这些模型完善，增加实际实施可行性，就是中国在区块链认知和普及上的一个巨大的进步。

以德勤为例，目前在全球已经形成了一个由世界顶级企业家，科学家，技术专家组成的专业团队，专门致力于探索开发区块链在金融和其他领域的应用。其中，DC3（德勤加密货币社区），Rubix（德勤自主开发的区块链实施和验证平台）团队，以及 Grid 团队都是全球区块链研究实施领域的佼佼者。德勤与美国奇点大学， MIT 数字货币实验室以及世界经贸组织都形成了合作伙伴关系，进一步研究和开发区块链的技术发展和实际商业场景应用案例。我们期待和中国的监管者，商界领袖以及矿工们一起推动区块链在中国的应用和实施--假若以区块链为代表之一的去中心化，点对点的技术革命是第四次工业革命，我们认为中国一定是全球的“革命根据地”。

（作者：秦谊　德勤会计事务所亚太区投资管理行业领导合伙人）

区块链:从信息传递到价值传递

最近一年多来，区块链在国内外备受瞩目，成为了金融科技领域最受关注的热点。包括纳斯达克、花旗银行、瑞士联合银行、德勤在内的数十个著名金融机构都在开展区块链金融创新，同时涌现了一批专注于区块链的新兴创业公司，区块链在除金融之外的其它许多领域也有广阔应用前景。区块链之所以被认为具有颠覆性意义，是因为它第一次能够从技术层面建立去中心化信任，这将成为构建新型价值互联网络的基础设施，开启价值交换的新时代。本文着重探讨区块链技术的关键意义，区块链如何构建去中心化信任，以及所面临的一些技术和应用层面挑战。

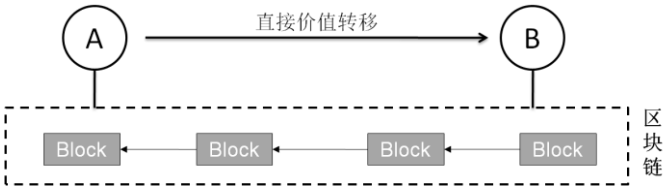
一、区块链技术的关键意义

今天的互联网，已经近乎完美地解决了信息传递，人们可以非常便捷、低成本地传递信息，然而，还不能实现点对点的价值传递，仍然依赖于中心机构承担记账功能，因为价值传递需要保证权属的唯一性，这不同于信息传递的可复制特征。简单地说，在信息传递之后，发送方和接收方能够同时拥有信息；但是，在价值传递之后，只能受让方拥有价值，转让方不能再拥有，目前这个转移过程的权属记录通过中心机构记账实现。那么，如果网络本身能够提供可靠的记账功能，将使得价值传递不再依赖于中心机构，直接进行点对点价值转移。

区块链就是一种分布式共享记账技术，它通过建立去中心化信任，实现不依赖于单个中心机构的记账，从而支持直接进行价值交换。如

图 1 所示，在传统模式下，从 A 到 B 转移价值的过程，需要中心机构参与记账；在区块链模式下，从 A 到 B 将能够直接转移价值，由区块链网络完成记账。

(a) 传统模式



(b) 区块链模式

图 1. 区块链的价值转移

区块链将有潜力使得互联网到达一个新高度，即从信息交换到价值交换，开创新一代价值互联网体系（Internet of Value），将极大地降低交易成本，对商业模式和经济社会产生重大变革。区块链支撑价值互联网，就如同 HTTP 等协议支撑信息互联网一样。

二、区块链如何建立去中心化信任

区块链交易处理与传统模式存在很大差异。在传统模式下，交易请求被直接提交给中心化系统，由中心化系统负责校验和结算等。在区块链模式下，如图 2 所示，在利用私钥签名创建交易之后，交易会被通过 P2P 网络传播，然后经过共识机制对交易进行验证，验证结果也通过 P2P 网络传播，最后，各个记账节点依据验证结果把交易写入账本。这就实现了分布式共享记账，交易验证、记账节点都不是单一中心。

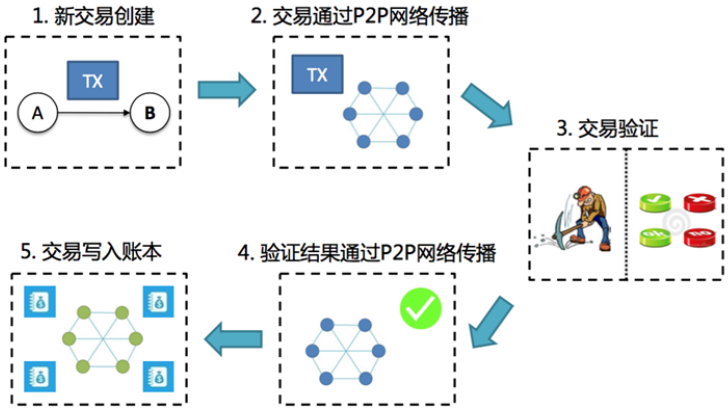


图 2. 区块链的分布式记账流程

区块链的技术实现，主要解决三个关键问题：分布式动态组网、时间有序不可篡改的密码学账本、统一规则下的共识机制，具体表现在如下：

首先，分布式动态组网。区块链的参与节点是多个，每个节点存在加入/退出的变化，因此，需要维护它们的动态连接关系，使它们组成一个网络。目前，区块链使用 P2P 技术来实现这一需求，P2P 技术是一项成熟技术，之前已被广泛应用在文件下载、视频分发等领域。

其次，时间有序不可篡改的密码学账本。区块链的账本结构，重点包含两个方面：（1）采用链式 Hash 结构实现防篡改，并提高账本之间比对的效率。由一串数据区块组成链，每个区块包含了前一个区块的 Hash 值，每个区块也包含了最近交易集合的 Hash 值。Hash 值可以看作是数据的指纹，数据的任何改动，都会产生新的结果，能够立刻被识别。（2）采用公钥密码机制标识资产所有者。区块链账本利用所有者的公钥作为账户标识，从而，仅持有对应私钥的用户才能对外转移资产。

最后，统一规则下的共识机制。共识机制是区块链技术的核心，它承担了交易验证和确认的功能，目的是解决双重支付问题，确保交易的唯一性。区块链的共识机制，既需要解决传统分布式一致性问题，维持全网节点账本的统一，还需要进行交易验证，以抵抗恶意攻击，确保交易的正确性。目前，在共识机制的实现上，比特币系统采用工作量证明方法，俗称“挖矿”；正在被广泛应用于金融领域的区块链共识机制，采用由部分节点作为共识节点，共识节点负责交易验证和确认，依据不同应用场景，在选择这些共识节点时存在不同的策略。

三、区块链面临的一些挑战

作为一项新兴的互联网技术，尽管具有巨大的应用潜力，但是，面对不同行业不同领域的场景，也存在着技术和业务层面的诸多挑战，这些挑战主要体现在如下几个方面：

第一，可证明的安全性。毋庸置疑，安全性是区块链技术的重中之重，涉及密码学算法的选取，尤其是共识机制的安全性。目前，虽然已有多种共识机制被提出，但大多数都缺乏严格的安全性证明，如何从理论和实践上证明共识机制安全性，是后续区块链发展的技术难点。

第二，共识机制的处理效率。共识机制效率与去中心化程度是个两难问题，需要根据具体应用场景进行均衡，去中心化程度越高，会导致共识机制效率降低。共识机制的效率，决定了交易处理时延和交易吞吐量，这是交易系统最关键的两个性能指标。

第三，海量账本的处理效率。随着用户数和交易记录量越来越多，

区块链的账本会越来越大，为了满足上层业务性能要求，需要改进账本存储策略和访问机制。同时，账本的规模化增长，会提高参与节点的硬件资源门槛。

第四，区块链与已有系统的结合问题。区块链作为一项基础设施技术，在实际应用中，往往都会遇到与已有业务系统的结合问题，这涉及到系统改造风险。所以，区块链前期主要应用于增量型业务的应用场景，随着技术越来越成熟，逐步渗透到核心业务。

第五，标准化的问题。众所周知，标准化是促进行业技术发展的重要推动力，它能够在整体上提高互连互通的能力。由于区块链涉及分布式协议和密码学等多项技术，解决方案多样，而不是单一的协议，因此，区块链技术的标准化过程可能会比较漫长。

第六，区块链生态系统的建立。区块链技术的分布式多中心特性，决定它往往应用于多方协作共享的场景，这是一个生态系统更迭的过程，常常关系到参与方原系统和业务的工作方式。因此，与区块链应用相关的生态系统的建立，将变得较为复杂。

第七，政策和监管。目前来看，区块链直接适用的是金融领域，而金融领域是有着严格法律监管的，区块链在重塑业务模式时，必须确保合规性。当前美国的几个典型区块链金融应用，都在合规性方面做了大量的工作。

（作者：蒋海　中国科学院博士、布比网络创始人）

研究团队主要成员

杨涛 支付清算研究中心 主任 研究员

程炼 支付清算研究中心 副主任 研究员

尹中立 支付清算研究中心 副主任 副研究员

费兆奇 支付清算研究中心 秘书长 副研究员

董昀 支付清算研究中心 副秘书长 副研究员

周莉萍 支付清算研究中心 副秘书长 副研究员

李鑫 支付清算研究中心 副秘书长 博士后

经邦 支付清算研究中心 特约研究员

宗涛 支付清算研究中心 特约研究员

徐超 支付清算研究中心 特约研究员

郭强 支付清算研究中心 特约研究员

主 办： 中国社会科学院金融研究所支付清算研究中心

主 编： 杨 涛 （ytifb@cass.org.cn）

副主编：程 炼 （clifb@cass.org.cn）

声 明

《支付清算评论》为内部交流刊物，其中的文章除非经特别注明，均由中国社科院金融所支付清算研究中心（以下简称“研究中心”）的研究团队完成，研究报告中的观点、内容、结论仅供参考，研究中心不承担任何单位或个人因使用本信息材料而产生的任何责任。本刊物的文字内容归研究中心所有，任何单位及个人未经许可，不得擅自转载使用。

研究中心是由中国社会科学院批准设立的所级非实体性研究单位，由中国社会科学院金融研究所作为主管单位，专门从事支付清算理论、政策、行业、技术等方面的重大问题研究。

研究中心的名誉理事长、学术委员会主席为中国社科院原副院长、国家金融与发展实验室理事长李扬研究员，理事长为中国社科院金融所所长王国刚研究员，常务副理事长为中国社科院金融所副所长殷剑峰研究员，主任为中国社科院金融所所长助理杨涛研究员。

地址：北京市朝阳区曙光西里 28 号中冶大厦 11 层中国社会科学院金融研究所

邮编：100028

电话：010-59868209，59868204

传真：010-59868203

E-mail：rcps@cass.org.cn

网址：www.rcps.org.cn

联系人：齐孟华

手机：13466582048