区块链技术在金融领域的研究现状及创新趋势分析[1]

近期，“区块链”成为全球金融业关注的热门词汇。2015年9月，摩根大通、巴克莱银行、高盛集团、西班牙BBVA银行、澳洲联邦银行、瑞士信贷集团、道富银行、苏格兰皇家银行和瑞士银行等九家全球知名金融机构，共同投资初创型公司“R3”，委托其为区块链技术在银行业的使用制定行业标准和协议。截止12月7日，已有包括富国、花旗、汇丰、三菱UFJ等在内的全球42家大型商业银行（金融集团）加入R3区块链计划，涵盖欧

[1] 本文为11月3日博士后工作站王硕赴央行做主题为《区块链技术在金融领域应用和研究的一些思考》学术交流的文字稿。

洲、北美、澳洲和日本等地区。可以说，区块链技术将有极大可能改变全球银行业的未来。

一、什么是区块链？

（一）区块链的概念和定义

2008 年，区块链（Block Chain）的概念由中本聪在论文《比特币：一种点对点的电子现金系统（Bitcoin: A Peer-to-Peer Electronic Cash System）》中首次提出，**业内普遍把比特币视为区块链在全球的首个应用**。

目前，全球对区块链并没有一个官方公认的定义。维基百科上“Block Chain”，直译过来就是“由比特币衍生出的一种加密货币序列交易的数据库技术”。综合国内外各方观点，个人认为，**区块链是指以去中心化和去信任的方式，借助数学算法集体生成一系列有序数据块，并由其构成一个可靠数据库的技术**。

（二）数据区块的要素构成和链接方式

区块链技术主要是让参与系统中的任意节点，使用密码学方法产生相关联的数据块（Block），并且生成秘钥用于验证其数据的有效性和链接下一个数据块。其中，**每个节点由一系列存储全网信息的数据区块链接而成**，如比特币系统中的每个区块存储的是某一时间段的全球比特币全部交易数据，每 10 分钟通过算法，生产新的模块，以此类推，滚动记录交易信息。

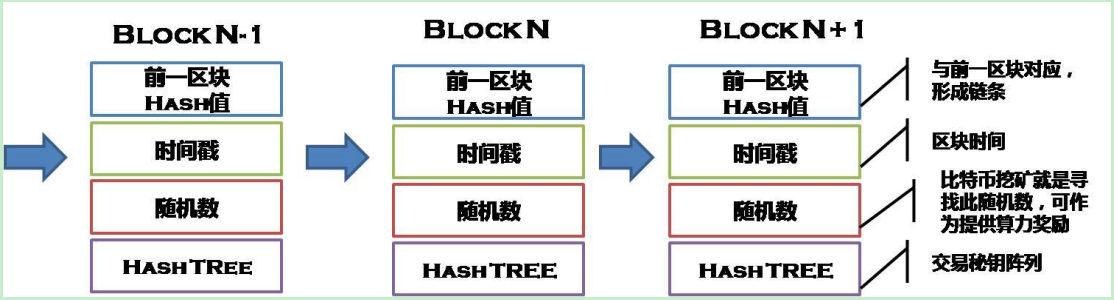

图 1 区块链结构与要素示意图

具体分析，每个数据区块由四个关键要素构成，分别是前一区块的哈希值、本区块的时间戳、一个随机数和本区块的哈希值树。其中，前一块的哈希值用于将本区块与前一区块构建映射关系，头尾对应成链；时间戳用于记录存储模块的时间段;随机数可用于挖矿奖励，激励各方参与，同时也提供了系统需要的计算能力；哈希值树是该模块下各类存储信息的秘钥阵列，客户只有密码才能获取数据区块下的某部分信息。总之，**区块链技术以加密算法为基础，通过去中心化的链条相通、时间有序，构建起记录和更新交易信息的全球分布式可信网络数据库。**

二、区块链的特点分析-以金融支付业务为例

（一）传统支付模式的特点-中心化

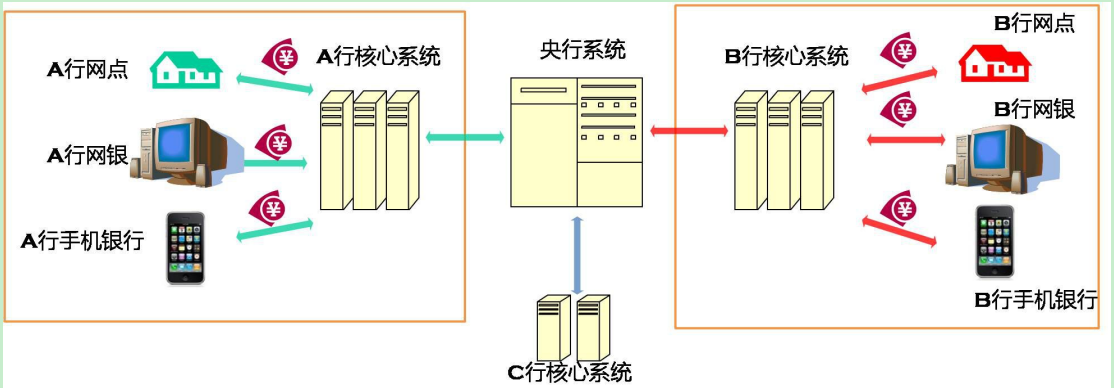

图 2 基于信任的中心化数据交互模式

图 2 是一个传统银行支付业务的数据交互示意图，当 A 行客户通过网点、网银、手机发生行内转帐交易时，信息传导到总部的数据中心，由其完成信息登记和资金划转，而客户的资金、账户等信息，都存在基于信任的 A 行核心系统服务器上。从 A 行视角看，这是一个典型的总分行中心化模式，A 行核心系统的服务器就是中心节点。同理，当 A 行客户跨行转账到 B 行，则需要通过 A 行核心系统-央行系统-B 行核心系统的信息传导路径，从整体流程看，央行成为交易的中心。可以说，**这种中心化模式是目前国内乃至全球金融交易的基本模式。**

（二）区块链支付模式的最大特点-去中心化

不同于传统的中心化的模式，**区块链是一种典型的去中心化的模式。**每个电脑主机都是一个平等的节点，系统中各个节点可以直接交互，没有中心节点概念。同时，任意两个节点的交易信息都向全网加密传播，所有节点都以加密区块存储方式、按时间序列单独记录系统全部交易信息，进而形成一种全新的去中心化模式。

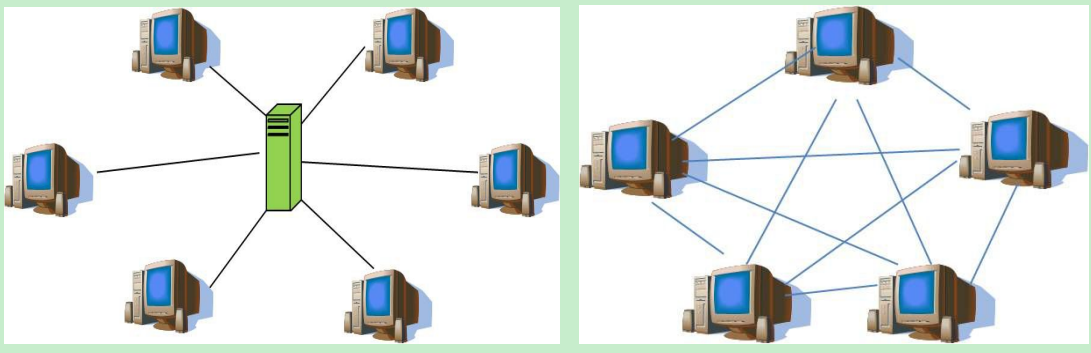

图 3 中心化模式与去中心化模式对比

具体分析，区块链技术具有四个主要特点。**一是去中心化。**

没有中心核心系统，没有一个中央的支付清算机构，节点间直接信息交互，任一节点损坏（系统升级或管制）不会影响全网运行，**交易效率高，成本低，业务连续性大大提升**。如希腊金融危机期间，监管当局一度将人均每日取款限额限制在60欧元，但在雅典街头的比特币取款机，由于采用了去中心化的模式，不受监管当局限制，居民可自由取款，不受限额约束。**二是去信任化。**不同于传统基于政府信用或法律法规强制的信任模式，而是借助开源算法，使得系统运作规则公开透明。在这种模式下，每个节点之间进行数据交换是无需互相信任，可以匿名，同时每笔交易都会被真实记录，以防止数据被控制和篡改，可以有效避免信任主体的违规行为（比如美国和俄罗斯的银行业可以匿名点对点直接交易）。**三是集体维护。**支撑金融系统的交易，需要庞大的计算能力。从区块链本身看，单个机器计算能力可能不高，但通过分布式点对点模式，使得计算能力大大提升，如现在比特币挖矿机的整体计算能力，已超过全球top500大型服务器计算能力之和的9倍，这个模式和国内网商银行金融云的核心系统架构理念相似，也是互联网“众筹、众包、合作、分享”精神的体现。**四是安全数据库。**单个节点可能会被暴力修改，但因为交易数据是分散到全网各个节点，单个节点的数据修改不被全网认可的。理论上分析，只要不是控制超过全系统50%以上的计算能力，数据是无法篡改的，而参与系统中的节点越多，计算能力越强，数据安全性越高。

三、区块链在金融（银行）领域的研究和应用现状

从国内外实践来看，除了在虚拟货币已开展实际应用外，区块链技术在金融领域，仍以探索性实验为主。但该技术在简化清算过程、降低交易成本上的巨大潜力，让众多金融机构，特别是商业银行为之侧目，并以支付业务为重点开展了一系列探索和研究。

（一）全球银行业区块链探索与研究情况

目前，包括**摩根大通、西班牙 BBVA、高盛、瑞银、桑坦德银行等一大批国际先进同业，或通过自身的创新实验室和产品孵化器，或采用股权投资方式，开展区块链探索实验和技术储备（见表 1）。**如花旗银行通过其创新实验室，创新出一种名为“花旗币（Citicoin）”的加密货币，现已开发了 3 条区块链。西班牙 BBVA 银行在 2015 年 1 月，通过旗下子公司以股权创投的方式参与了 Coinbase 融资；7 月，BBVA 宣布将在区块链技术基础上，建立完全去中心化的金融系统思路。瑞银 UBS 集团于 2014 年在伦敦成立了区块链金融研发实验室，重点探索区块链在支付、电子货币和结算模式等方面的应用前景。桑坦德银行在 2015 年 6 月，通过金融技术投资基金 InnoVentures 进行区块链试验，研究如何将区块链技术应用于传统银行业，目前已发现了 20-25 种场景，并认为该技术每年可节省 200 亿美元的国际交易结算成本。此外，包括澳大利亚联邦银行、西太平洋银行（澳洲）、荷兰银行、荷兰安智银行（ING bank）、拉博银行、星展银行等多

家银行，都已开展区块链技术的应用探索。

表 1 区块链技术在部分银行的研究现状

银行	研究现状
花旗银行	在其创新实验室一直探索“花旗币”（虚拟电子货币）的实验项目，目前已开发了 3 条区块链，并开始内测。
西班牙对外银行（ BBVA）	1 月，通过旗下子公司以股权创投的方式参与了 Coinbase 融资；7 月，BBVA 宣布将在区块链技术基础上，提出了完全去中心化金融系统的构建设想。
瑞银（UBS）集团	2014 年，瑞银就在伦敦成立了区块链金融研发实验室，重点探索区块链在支付、电子货币和结算模式等方面商业银行领域的应用。
桑坦德银行	6 月，通过金融技术投资基金 InnoVentures 进行区块链试验，研究如何将区块链技术应用于传统银行业，目前已发现了 20-25 种可以使用区块链的场景。桑坦德认为，区块链技术或许能实现每年节省 200 亿美元的国际交易及结算成本
巴克莱银行	通过“巴克莱加速器” 选出了三个区块链相关的初创公司 Safello，Atlas Card 和 Blocktrace 开展投资孵化。6 月，巴克莱银行与比特币交易所 Safello 开始联合探索区块链技术如何服务传统金融业。
纽约梅隆银行	尝试将比特币的点对点模型基础到银行系统，并在其员工内部系统中推出 BK Coins 虚拟货币
美国 Cross River 银行等	美国的 Cross River 银行、CBW 银行以及德国 Fidor 银行，与数字货币公司 Ripple Labs 合作，以虚拟货币作为媒介，开展跨境汇款服务实验。

注：来源于网络公开信息整理

（二）全球银行业初期关注点在支付领域

全球银行业对区块链技术的初期关注点，主要集中于支付领域。目前，国内的支付关键系统，包括央行大小额系统、各银行自身核心系统、银联系统等，是一种典型中心化的模式，而跨行交易手续费较高，大额交易时间长，某个系统关闭或者出错，会导致交易无法实现。跨境支付更是需要借助 swift 等在各个银行、代理行之间进行交互，节点多、流程长、效率低、成本高，易出错。但如果采用区块链技术，使用分布式核算，而非由第三

方中心管理，所有交易都实时记录在类似于全球共享的电子表格平台上（数据通过加密无法破译和篡改），只要不全球断网断电，每一用户都能凭密查询交易状态，资金实时清算，效率大大提升。

表 2 国际贸易支付模式费率和效率对比

业务模式	费用	到账时间	其他问题
电汇（T/T）	手续费：0.1%（美元）；电报费：100 元 RMB；外币转换费：1%-3%	一般 1-3 天	没有追踪汇款状态的直接途径
西联汇款	<500 美元(15 美元)；500-1000 美元(20 美元)；1000-2000 美元(25 美元)；2000-5000 美元（30 美元）。	一般小于 30 分钟	单笔额度受限制，小额转账成本高
比特币支付	零费率将人民币转换成比特币，兑换外币取决于不同平台和币种手续费（0-3%）	秒级	目前没有大规模应用

注：不同银行收费标准存在差异

具体来看，以国际支付为例，除了传统的卡模式外，电汇和西联汇款是两大跨境支付的重要模式。如表 2 对比所示，电汇适合大额汇款，手续费稍低，但到账时间较长，且由于采用代理行模式，很难了解具体进程。西联汇款时间比较快，但额度受限，且收费较高。与传统国际支付模式相比，采用应用区块链技术的虚拟货币转接进行支付，额度不受限制，可实现秒级到账，且手续费极低，这正是区块链技术大量吸引国际银行业参与其中的关键。本质上，**各家商业银行希望利用区块链技术，在解决互信的基础上，构建扁平化的全球一体化清算体系，突破现有的系统间割裂的现状，以及额度等监管限制，降低成本。**

（三）区块链在审计、数字资产等领域应用刚刚起步

除了支付领域，金融业对于区块链技术在审计、数字资产、信用体系建设等方面也开展一些探索。如德勤利用区块链技术中信息可追溯、不易篡改的特性，构建了 Rubix 基础平台，通过与核心客户的 sap、oracle 等数据库对接，自动获取并记录客户财务信息，防止篡改或伪造财务报表。部分专家也提出，可以将房产等实物资产以电子权证方式存储在区块链上，并借此开展全球金融信用服务等。

在国外金融同业对区块链技术研究如火如荼的同时，国内对区块链技术也开展了一些研究工作，主要集中在**清华大学**等高校、**阿里巴巴、万向集团**等企业巨头以及部分初创型公司，以**虚拟货币类**的实验探索和理论研究为主。

四、区块链未来的发展前景和需要关注的问题

技术进步、监管套利和市场需求变化是金融创新的三大重要动力。随着区块链技术的日益成熟，以及全球各方所倾注的热情，未来区块链技术将极有可能改变我们的生产、生活和社会规则。

（一）区块链技术的应用前景

从趋势上分析，区块链技术应用前景可以分为 1.0、2.0 和 3.0 三个阶段。在 1.0 阶段，**主要是以支付为突破口，通过区块链技术构建全球一体化低成本的实时清算体系，目前全球正处以这个阶段的萌芽期**；在 2.0 阶段，主要是以数字资产、智能合约等为代表，从单纯的支付环节向后端的资产和信用领域拓展；在 3.0 阶段，区块链技术将有可能在政府财务监督、科学文化等领

域产生深远影响。

（二）区块链技术应关注的几个问题

一是监管难题。区块链去中心化、可追溯、匿名性的特点，对金融监管技术和模式带来全新挑战。在区块链技术下，由于没有中心系统，很难锁定客户的多个匿名账户，除非掌握秘钥，否则很难了解资金去向，这极可能被犯罪分子利用,带来洗钱、诈骗、偷漏税等一系列监管新难题。**目前，各国监管当局，对于区块链技术发展仍处于观望态度。**

二是各个国家的差异化认识。采用某种虚拟货币作为等价物进而实现全球一体化的实时清算，某种意义上说，对各国央行的实体货币和发钞权本身就是一种挑战。实体货币是国家以自身信用为背书并由此获得铸币税，但虚拟货币的信用就是数学算法，很难体现单一国家的金融意志。作为清算标的，虚拟货币在一定程度上很可能替代本币，这是很多国家无法接受的。以比特币为例，目前，德国等国家承认比特币的合法货币地位，但大部分国家仍将其视为大宗商品，无法接受其货币属性，各个国家对此认识不同是该技术在金融领域应用需要关注的问题之一。

三是技术发展的问题。虽然区块链的技术逻辑清晰，理论上很难被暴力破解，但通过挟持大批僵尸机，或采用工会集群运作模式，仍有篡改数据的可能，比如全球最大的比特币工会控制的算力已达全球比特币算力的 42%，距离 50%只有一步之遥，一旦区块链应用范围和金额扩大，黑客等技术风险必须予以关注。

四是民众的接受程度。目前，在全球很多地区居民还是习惯使用现金和银行卡，民众还是信任有实体网点的商业银行，而对于将自身交易信息乃至资产，上传到纯粹基于加密算法作为基础的网络区块链上，民众内心接受将是一个长期艰难的历程。

五、结语

无论如何，区块链技术代表了未来信息数据存储和交互的重要技术发展方向。虽然无法断言虚拟货币将来会完全替代法定货币，但随着互联网金融的升级，以及 P2P 等去中介化新兴模式的发展，在全球大型金融机构联合创新推动下，区块链技术正从概念走向应用。**我国银行业也应高度关注国际同业最新创新动向，积极参与一些标准制定和前瞻性创新，实现由跟随型向引领型创新的转变。**

展望未来，虽然面临技术、政府监管和法律等方面的诸多挑战，但正如 1792 年的《梧桐树协议》奠定了金融业自律发展的基石，利用新技术降低金融交易成本、减少信息不对称永远是金融业创新的方向。