区块链技术在金融领域的应用解析

文 ‖ 北京航空航天大学　蔡维德
北京大学　郁莲

蔡维德，北京航空航天大学千人计划教授；北京航空航天大学工信部工业和信息化法治战略与管理重点实验室高级研究员；计算法律学专家；亚利桑那州立大学名誉教授；OW2（中国—欧盟开源软件联盟）副理事长；麻省理工学院学士，加州大学伯克利分校博士。

言及区块链技术，人们往往会联想到加密货币、加密算法、点对点协议、投票机制、分布式总账等。但银行是否可以应用全部区块链技术？本文将加以研讨，并从软件和硬件出发，系统阐述区块链技术在金融领域的应用，并为数字货币的发行提供参考。

各金融机构对区块链技术的态度

当今诸多金融机构及社会组织均表示支持区块链技术，英国首席科学顾问代表英国官方于 2016 年发布白皮书，提出：

★分布式账簿算法具有颠覆性的创新，可以改转公共和私有服务，并通过广泛的应用提高生产力。

★区块链技术应该首先在政府进行初步尝试。英国政府建议由部长主导建立政府内部的区块链技术平台，将“政府数字服务”作为政府管理机构，建立区块链技术愿景和路线图。

★英国研究机构强调应进一步强化投资基础研究，以保证分布式账簿的安全性、可扩展性，并提供其内容的正确性证明。

★英国政府需要进一步考虑如何建立“分布式账簿技术的监管框架”，监管框架需要和区块链技术的实现和应用并行发展。

★英国政府呼唤与学术界和工业界合作，并确保针对“分布式账簿及其内容的完整性、安全性和隐私性”建立可参考的标准。标准包括监管要求以及软件代码。

★英国政府需要在政府内部发展能力和技能。并培养一个跨政府的利益共同体，聚集各种分析和政策团体，产生和发展使用案例、专业知识体系。

值得注意的是当前诸多金融机构仍对区块链技术持保留态度，例如欧洲债券结算系统（Euroclear）、美国存管信托和结算公司（DTCC）以及瑞波思想（Ripple Insight）。

Euroclear 最近发布了白皮书《资本市场的区块链技术》，认为区块链技术只有在确保可以解决实际问题后才能被广泛接受，目前现有的技术如中央证券托管具有与区块链技术相同的功能。

DTCC 认为区块链技术：没有改进现有对数据的检索、查询或分析等技术；没有与现代数据库一样的数据搜索技术；没有提供高速访问数据和数据分析的技术；没有整合现今的数据管理工具；没有解决大多数处理系统的非功能性需求。同时他们认为尽管区块链技术可能大幅提高结算效率，但需考虑的问题仍很多，例如配套的法律机制、市场的认可、资产管理

郁莲，北京大学软件与微电子学院副教授，从事软件分析与验证、分布式系统架构等教学与科研。清华大学经济管理学院管理信息系统系硕士，日本国立横滨大学情报工学博士。

以及投资者的保护等；而且使用分布式账本的方式进行结算，需要大量资金。

瑞波思想认为，人们会发觉单纯的区块链技术并无意义，必须发挥其在某个行业的应用作用，而将其应用于金融业似乎十分可行。他们认为当前技术的产业支持、风险管理机制、监管方式和对遗留系统的兼容非常完备，多数区块链专家所倡导的区块链的应用价值仅仅是技术探讨，尚未达到实际应用程度。这讨论决不可囿于技术本身，而应当强调其应用属性。

金融区块链应用需求

本文综合考虑了 Euroclear、DTCC 和国际结算银行（BIS）发布的白皮书，提出了金融区块链技术系统的需求，即未来数字货币发行必须监管的若干问题。

值得关注的是，当前的区块链技术远远达不到处理金融交易的要求。原因在于很多加密货币仍没有解决监管问题。

BIS 详细列举了监管数字货币的关键方法：信息 / 道德劝告，如公共预警；利益相关者监管，如数字货币局或交易所监管；完备的法律机制，通过法律解释如何监管数字货币；适当的监管机构；配套的监管方式，如禁止使用数字货币进行零售交易。

欧洲银行联盟（European Banking Federation，EBF）针对如何使用加密货币建议：政府部门配合行业参与者对加密技术的影响进行评估；建立良好的监管方法，确保用户对加密技术的信赖；强化对交易行为的监管，参见反洗钱和反融资。并强调以一个系统的方法来解决这些问题。

我们知道，金融系统有高吞吐量和低延迟、安全和隐私、合规性、可靠性和持续性等要求，而交易系统的恢复能力更是共同需求。针对数字货币，BIS 提出了其需求在于包括商业模式的可持续性、安全性、可扩展性。同样，效率、成本、可用性、跨国界、隐私、营销信誉等关键要求都应当涵摄进来。

金融区块链技术的设计

当前区块链技术的设计主要包括这几个关键要素：级联加密、时间戳、P2P 网络、挖矿、多份独立副本、数字货币。在数据货币方面，如果区块链技术中的账本表示资产，那么账本可以用来发布数字货币并进行金融交易。费利克斯·马丁解释说，“分布式的账本”可以创建数字货币，不是“挖矿机制”创建货币。最早的“数字货币”出现在 16 世纪的欧洲，当时的“分布式的账本”是保存在银行系统中，而不是在某种电子数字媒介中，银行家手动维持账本一致性。当前数字货币（加密货币）是存在于电子数字媒介中。如比特币用挖矿机制来维持分布式账本的一致性，这种协议的劣势在于速度很慢。区块链技术可以使用其他方法维持账本的一致性，为数字货币发行可验证提供了一定的准则，例如使用拜占庭容错协议（Practical Byzantine Fault Tolerance，PBFT）。

这些特征出现在第一代加密货币，即比特币，以及第二代加密货币，如瑞波币、比特股和以太坊。如今，新的区块链技术有不同的设计：超级账本项目由 Linux 基金会发起；Hydrachain 是以太坊的私有区块链技术，它有不一样的设计；北航链是一种新的私有区块链技术。

笔者认为，对于区块链在金融领域尤其是数字货币的应用监管，可信赖的安全性、隐私的强化保障和性能的提升（速度等）是关键。

1. 首先应该有完备的加密机制和可信赖的时间戳：金融区块链技术需保护交易的隐私性，因此要额外增加安全和隐私机制。

2.P2P 网络 /P2P 计算：其可以简单定义为通过直接交换来共享计算机资源和服务，而对等计算模型应用层形成的网络通常称为“对等网络”。P2P 网络操作具有匿名、非中心化的特点，在 P2P 网络环境中，成千上万台彼此连接的计算机都处于对等的地位，整个网络一般不依赖专用的集中服务器。网络中的每一台计算机既能充当网络服务的请求者，又对其他计算机的请求做出响应，提供资源和服务。通常这些资源和服务包括：信息的共享和交换、计算资源（如 CPU 的共享）、存储共享（如缓存和磁盘空间的使用）等。P2P 网络环境下的每个节点既是客户端也可以是服务器，多路径的连接使得 P2P 网络很好地保障用户隐私。但多节点的特性使得 P2P 网络比一般网络慢。虽然 P2P 网络有极强的容错性，但这一特性却极易导致网络低性能。

P2P 网络匿名、多中心的属性使其可以有效避免政府监管，当前频发的版权侵犯（以快播案为例）、安全漏洞等问题已经严重影响了 P2P 技术的形象。同样，基于 P2P 网络产生的比特币存在安全性、洗钱等问题。P2P 网络 Napster 的创始人肖恩·范宁提到他创建 Napster 的初衷是“用户建立一个虚拟的网络，在物理位置上完全独立，不必服从任何权力单位的监管及限制。”可见，P2P 网络的设计目标是避免所

图 1　可靠性分析

有权力单位的监管。这里就会出现一个悖论，P2P 网络不接受国家、省、市、地方政府和公安等的监管，与金融系统的设计目标“强制监管”显然互相矛盾。

笔者认为，在构架金融系统的时候，其基础网络不应当采用 P2P 技术。因为对于涉及国家命脉的金融行业，有效监管仍必不可少，但在解决数据库、云平台、金融系统容错性时，则可以对 P2P 技术加以扬弃。以亚马逊的分布式存储引擎 Amazon Dynamo 为例，它正是用于 P2P 网络技术而充分保证容错性和稳定性。P2P 网络的容错性，保证了任何部分系统出现故障都不会影响整个网络或丢失数据，一定程度保障了数据安全。

3. 挖矿：如果不使用 P2P 网络，则不再需要奖励机制。由参与的银行来维持账本，只需要一致性协议来实现账本的一致性。

4. 数字货币：中央银行注重用户支付和操作时存在的风险问题。欧洲银行协会已配套团队开始专门研发分布式账本（对是否产生数字货币尚在考虑中），区块链技术的应用使其可以用分布式账本来追踪现金流、股票、债券等数字资产，并非常便捷地清算双方的资产。这也为数字货币的发行提供了可能性，区块链技术以及数字资产可用于金融领域，不仅仅是数字货币，同样包括外汇、汇款、实时支付、跟单贸易和资产服务等结算。

5. 多份独立副本：当前银行业的账本一般只有副本，这显然是传统的中心化系统。世界许多中央银行就是用中心化系统，商业银行需要在央行进行结算。由于所有的数据流只有一个中心，对监管而言显然更行之有效。但从另一个角度来看，这极大地限制了数据的流动性，会带来两个显而易见的问题：抵押品的交换几无可能；一旦有区域发生经济危机，当地银行及公司都将受到打击，且容易感染其他地区和领域的经济。

这种中心系统必须提供绝对的信赖感，任何故障或非法操作都将导致严重后果。而放弃中心化的劣势在于使用多个副本，在通信、计算和存储方面将消耗大量资源，每次操作都需要执行一致性算法且数据要存储多次，这些行为以及大量的交易都表现在金融系统中。此外，许多一致性协议是以串行的方式执行，即使增加额外的处理器和宽带也很难加快一致性协议的速度。

不能忽视的是，多副本会增加系统的可靠性和安全性。例如，拜占庭协议可以容忍区块链技术中少于 1/3 的节点失败。图 1 显示了在给定的节点失败概率和节点数的情况下，区块链技术的平均使用寿命。水平轴表示节点数，垂直轴 Years 表示超过 1 / 3 节点失败时区块链技术的使用时间。

表 1　区块链设计总结

	原始区块链技术	金融区块链技术
加密和级联加密	是，交易信息是公开的	是，交易信息是私有的
时间戳	是	是
多份独立副本	是，P2P 网络中所有节点都参与	是，需要选择节点的数目
网络	P2P 网络	高速网络
挖矿	是，如 POW	改用一致性协议
数字货币	是	是，但非必需

表 2　Hydrachain 和北航链的特点对比

特点	HydraChain	北航链
块的创建	一个领导者创建一个新的块	任何节点可以创建新的块
投票	每一个新的块；拜占庭式投票	每一个交易、新的块和块的投票结果；拜占庭式投票
投票失败处理	如果收到 1 / 3 投票，则再次投票	每个交易至少有 n（现在是 5）次机会被投票
交易数据加密	是	是
处理方式	顺序执行	投票和数据收集同时进行
领导者选择	轮询	多种策略
信誉系统	未采用	是，可识别作弊节点
速度	1K TPS	12K TPS
可扩展性	难	易

图2 Hydra-chain 的架构

Years $= 1/(\sum_{k=\frac{n}{3}+1}^{n} C_n^k p^k (1-p)^{n-k})/365$，其中 n 是节点个数，p 是节点失败的概率。

在节点每条出错概率为 0.01 的前提下，16 个和 31 个节点区块链系统崩溃的时间分别约为 372853 年和 3890 亿年。所以，区块链技术系统不需要很多节点就能保证可靠性。节点个数越多，系统越可靠，但也更慢。因为每次创建块，任何一种一致性协议都要求一个节点广播它的状态或者交易，将产生 O（N^2）个消息。

现有的私有区块链技术

1.Hydrachain。Hydrachain 是基于以太坊所架构的私有区块链技术（见图 2），它使用 PBFT 一致性算法而非挖矿机制，速度远超挖矿机制。

笔者曾与以太坊创始人 Vitalik Buterin 交谈发现只有 5% 的以太坊程序可被金融领域使用，其余 95% 的包括挖矿等在内的机制不仅不能帮助应用，反而使区块链速度变慢。此次研讨后，其团队开发了 Hydrachain，笔者团队则开发出北航链。虽然 Hydrachain 和北航链目标一致，但 Hydrachain 不愿抛弃以太坊已开发的大量软件，其软件仍在以太坊的架构上运行。这也导致了 Hydrachain 在金融领域使用的局限性。

图3 北航链的架构

2. 北航链。如图 3 所示，北航链是北京航空航天大学与北京大学联合开发的私有区块链技术，其设计初衷是为公信和金融服务，所以北航链抛弃了 P2P 网络和挖矿机制，以“可扩展性”为第一目标，并重视速度优化。为了确保系统安全，加入了节点信用制度。这是国内外首次采用信用机制来识别作弊节点，一旦发现节点的作弊行为立即将其排除在投票节点之外。

在北航链的设计中，拜占庭式投票和数据采集可同时进行，大幅加快了其信息处理过程，其自身具有独特的块的创建过程。此外，不只是对块投票，对每个交易也要投票。为了确保安全，也对块的创建结果投票，可以判断是否有叛徒节点。由于三轮投票，将产生更多的信息（每轮产生 O（N^2）个消息），由于其本质为并发操作，所以速度快。在某种特定配置中，北航链可达到 24K TPS。且这些是在没有硬件优化、负载均衡、数据重组及异步操作的情况下的结果。

另外，北航链还设计了一整套可扩展的机制，使得区块链能够有高吞吐性、低延迟性以及高隐私性。有了这样的机制，当工作量需求增加的时候，只要增加机器就能够处理。

区块链技术的应用使得数字货币的发行成为了可能，但是数字货币发行仍道阻且坚，应该首先解决区块链技术在金融领域应用存在的问题，再去细致考虑数字货币发行的问题。但要注意，互联网的自由主义思想不应该外化为社会生活的意识形态，二者应当分而治之。从社会发展尤其是金融行业发展角度出发，安全监管十分必要，数字货币的发行尤其如此。

参考资料：

[1] UK Government Chief Scientific Adviser, Distributed Ledger Technology: Beyond Block Chain, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf
[2] European Banking Federation, Driving the Digital Transformation: The EBF Blueprint on Digital Banking and Policy Change, http://www.ebfdigitalbanking.eu/EBFDB_3.html