DOI:10.19641/j.cnki.42-1290/f.2019.07.024

区块链金融应用场景的可延展性剖析

谢智勇(副教授)

【摘要】区块链金融应用中,网络结构、共识机制和激励机制是需要考虑的重要因素。区块链的网络结构主要有单链、侧链和链下网络等,能够有效解决金融应用中的数据高并发问题;区块链的共识机制在工作量证明机制的基础上,衍生出了权益证明机制和授权股权证明机制;竞争记账权的激励机制包括通证激励、手续费激励、保证金激励等。不同类型的网络结构、共识机制和激励机制可以相互组合,因此区块链的金融应用具有很强的可延展性,可以根据不同金融业务的特点,适当裁剪和组合区块链技术的主要功能,使之成为可靠的工具和平台。

【关键词】区块链;金融应用;网络结构;共识机制;激励机制;可延展性

【中图分类号】F812.42 【文献标识码】A 【文章编号】1004-0994(2019)07-0166-5

一、引言

2008年10月,匿名为中本聪的作者在一个密码论坛发表论文《Bitcoin: A Peer-to-Peer Electronic Cash System》,提出了区块链的主要原理和机制设计[1]。2009年1月,第一个区块链开源代码正式发布,第一批50枚比特币被挖掘出来。在去中心化基础架构与分布式处理范式基础上建立的区块链技术,具有可追溯、不可篡改、非对称加密等特征,有效地解决了市场交易中的拜占庭将军问题,能够作为经济和管理的可靠的工具和技术[2]。经过短短十年的发展,区块链技术已经得到了政府、企业和资本市场的广泛关注,以Bitcoin、Ethereum、Ripple为代表的公有链,以Hyperledger fabric、CITA为代表的联盟链等区块链应用快速发展起来。一枚比特币曾经达到近两万美元的价值,以太坊市值最高超过了1000亿美元。相关数字货币市值的波动,说明各种区块链应用还在不断尝试和完善的过程中。

在区块链的发展进程中,个别过度投机行为造成的误解在一定程度上掩盖了其作为技术架构的潜在价值。曾经发展很快的ICO(Initial Coin Offering)成为区块链发展过程中不恰当的诱因。国家互联网金融安全技术专家委员会发布的《2017上半年国内ICO发展情况报告》的数据显示,2017年1~7月,65个ICO项目累计融资规模将近26亿元人民币,与ICO相关的各类风险逐渐暴露。基于区块链工作量证明机制的算力竞赛一度成为追求收益的热点。工作量证明机制一般是要求计算一个无价值的散列值,需要消耗大量有价值的计算资源和能源,且较长的交易确认时间使其不太适合小额交易的商业应用[3],影响共识机制作用的发挥。但是,区块链的通证经济功能(Token Economy)具有广泛的借鉴意义。

2016年3月,高盛发布的研究报告《Blockchain: Putting Theory into Practice》,展示了区块链在共享经济、股票交易、再回购协议、杠杆贷款交易等方面应用的案例。曹淑艳等[4]对区块链相关文献的统计结果显示,我国85.3%的区块链研究集中在供应链金融、数字货币和互联网金融三个领域,国外83%的区块链研究面向金融系统的应用。区块链金融应用中,网络结构、共识机制和激励机制是需要考虑的重要因素,经过多年的探索,已经发展出了多种技术路线和相应的机制设计,可以根据各类金融业务的具体要求,把区块链的主要机制进行适当裁剪和组合,以适应不同层次的金融业务,有效实现区块链金融应用场景的可延展性。

二、区块链金融应用中网络结构的可延展性

区块链网络层采用P2P联网方式,节点间通信

过程不依赖中心化的第三方，每个节点具有相同地位，具备部分或全部的钱包、路由、区块记录和挖矿等功能[5]。各节点共同参与区块链运行中的信息广播、数据存储、交易验证等任务，具有去中心化、分布式、自治性和开放性等特点，即使部分节点遭受攻击，也不会影响整个系统的稳定运行。但是，一般区块链处理交易的速度比较慢，随着节点数量的不断增加和网络规模的不断扩大，区块链系统中信息传播的及时性可能会下降。一项对比特币网络的研究显示，信息传播时间随着区块大小呈线性增长趋势[6]。相对金融业务的数据高并发要求，传统的区块链网络结构制约性较大。例如，比特币系统每秒仅能处理7笔交易[7]，较快的区块链处理交易速度能够达到每秒数十笔。但是，相对于VISA每秒能处理2.4万笔交易的能力，显然不是同一个数量级。因此，区块链金融应用需要突破的第一个瓶颈就是扩容，解决的思路可以从网络结构的可延展性切入。

1. 单链。不借助区块链之外的信息单元，独立实现数据传输、验证和存储功能的区块链系统都可以称为“单链”，例如比特币、以太坊和莱特币的主链。单链可以是基于一致性哈希表构建每个节点的路由表而形成的结构性单链[8]，也可以是节点之间的路由靠广播的方式实现的无结构网络。单链式的网络结构，适用于对数据安全性要求高、交易活动频率低的金融业务。

2. 链下网络。金融业务场景通常由一系列数据变化的记录组成，数据处理过程具有持续性和高并发等特点，高速度和多数据处理能力是金融业务信息管理的重要条件。一些区块链发展出链下网络结构，提供互联网级别的并发支持，以满足包括各种交易分析、数据验证、海量存储等业务的需求。同时，通过链下网络设计，能够有效保护金融企业的数据资产，防止因区块链数据公开性引起的数据资产价值外溢而影响金融企业参与的积极性。

3. 侧链。侧链可以实现不同区块链系统之间的链接，提供跨区块链交易的解决方案，其运行建立在简单支付验证（Simplified Payment Verification，SPV）的基础上。SPV设计为动态成员多方签名，发生在基于工作量证明的主链上，包括展示工作量证明的区块头和特定项输出的密码学证明。有了SPV机制，不需全节点运行就可以验证支付信息，实现区块链之间的数据资产转移[9]。侧链技术的出现，为不同金融机构之间的交易提供了更大的空间。

综上，三种区块链网络结构的主要特征归纳如表1所示：

表1　　区块链网络结构的主要特征

网络结构类型	单链	链下网络	侧链
主要特征	单独运行的区块链	互联网级别的并发支持	跨区块链解决方案

三、区块链金融应用中共识机制的可延展性

区块链的去中心化特征带来了分布式一致性问题，计算机学科称之为共识算法或者共识协议，而经济学科称之为共识机制或证明机制，重点解决分布式集群系统中各节点数据的匹配性和交易的一致性。区块链中常用的共识机制包括工作量证明机制（Proof of Work，PoW）、权益证明机制（Proof of Stake，PoS）和授权股权证明机制（Delegated Proof of Stake，DPoS）。这些共识机制为金融业务的去中心化和弱中心化提供了多种可选项，从另一个层面体现了区块链金融应用的可延展性。

1. 工作量证明机制。对共识问题的研究最早可以追溯到Eisenberg、Gale[10]的论文。比特币系统最早采用的工作量证明机制被认为是安全可靠的公有链共识算法，其基本原理是各个节点利用自身的计算资源，试算一个难度大但易验证的数学难题，最快找到符合条件的随机数的节点，以获得下一区块的记账权并得到一定数量比特币的激励。这个过程被形象地称为“挖矿”[11]。工作量证明机制可以吸引众多节点参与，但也存在耗时长、能耗高的缺点，不能很好地适用于大部分金融业务场景。

2. 权益证明机制。2011年7月，匿名为Quantum Me-chanic的作者在比特币论坛提出了权益证明机制。2012年8月，Peercoin区块链系统正式采用权益证明机制。该机制的基本原理是要求节点依据所拥有的相应数字货币数量竞争区块链的记账权。为了防止由此带来的记账权的集中化，损害共识机制的公正性，不同区块链系统在权益证明的基础上，通过增加记账权的随机性来避免中心化。这种方式的优点是耗时短、能耗低，虽然存在信用基础较弱的缺点，但是可以与传统金融机构的信用担保功能相互倚重，适用的金融业务更加广泛。

3. 授权股权证明机制。2013年8月，比特股（Bitshares）项目首先采用了授权股权证明机制。授权股权证明机制的原理类似于投票选举董事会，区块链中各节点将持有的股份权益作为选票投给某个愿意承接记账任务的节点，获得选票最多的特定数量节

点进入“董事会”，在约定期限内轮流行使记账权。授权股权证明机制有效地解决了工作量证明机制资源浪费和权益证明机制可能的节点参与积极性不高等问题，确认速度更快。在实践中，为解决节点投票积极性不高的问题，还可以采用加密抽签的形式选择出“董事会”节点。

综上，三种区块链共识机制的主要特征归纳如表2所示：

表 2　　区块链共识机制的主要特征

共识机制类型	PoW	PoS	DPoS
主要特征	可以吸引更多用户参与，消耗过多的算力和能源	降低共识机制的成本，可能会影响共识机制的公正性	确认速度更快，存在投票积极性和安全性隐患

四、区块链金融应用中激励机制的可延展性

在区块链应用中，激励机制同样居于核心地位。通证激励对区块链激励机制的影响比较大，很多人把激励机制等同于通证激励，这种看法从逻辑上简单否定了激励机制的多样性和可扩展性。从公链的角度来看，双方在没有任何信任的基础上，激励机制就是通证激励，典型案例就是比特币系统。但是，区块链发展出了一个更广义的激励机制基础——智能合约，将金融业务链条中的关系、流程放到智能合约里，由此会产生更多的激励方式，如手续费激励、保证金激励。在智能合约里，可以根据数据和交易的贡献，决定回报的形式和数量。更广泛地，可以让不同参与方的交易和创新能力通过智能合约实现，而不是用简单的通证激励来解决。

1. 通证激励。目前，大多数公链所采用的激励方式是通证激励，虽然有些区块链在此基础上做了一些改进，但本质并没有改变。尤其是在我国，代币的性质和流通都受到了很大的约束，通证激励发挥作用的空间十分有限。区块链金融应用中，采用通证激励的可能性较小。

2. 手续费激励。比特币系统没有规定交易手续费的具体数额，该数额由交易数据和交易次数等因素决定。由于每个区块的数据容量的限制，挖矿者会优先记录手续费较高的交易。根据2017年比特币交易数据统计，手续费的平均比例为0.5%～1.5%，从绝对数额来看，每笔交易的手续费从2017年初的约10美元上升到约100美元。以手续费作为激励手段，与金融业务的交易标的性质相符，应用空间很大。

3. 保证金激励。区块链金融应用中，采用许可区块链形式的可能性更大。许可区块链中存在高权限节点，目的是维护规则和控制权限[12]。很多许可区块链的共识机制不以复杂算法为基础，易受攻击。在这种情况下，保证金机制可以发挥很大的作用，既能以负激励的方式防止节点作恶，也能以正激励的方式奖励举报作恶，并设计以保证金为基础的记账权奖励规则。

综上，三种区块链激励机制的主要特征归纳如表3所示：

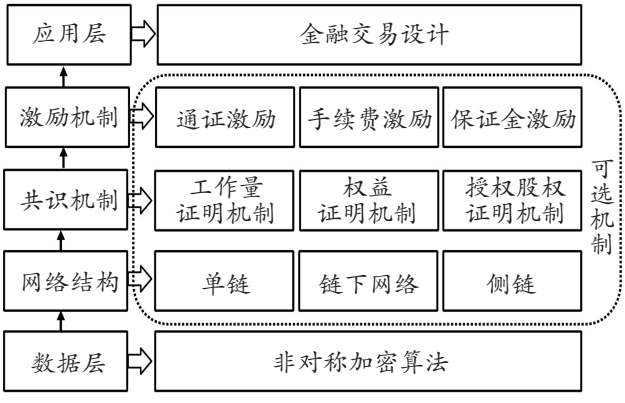
表 3　　区块链激励机制的主要特征

数据存储类型	通证激励	手续费激励	保证金激励
主要特征	成本低、易操作、制约因素多	易操作、成本高	兼具正负激励效应

五、区块链金融应用的适用选择

因为区块链肇始于比特币系统，很多人形成了区块链单链式公链、工作量证明机制和代币激励的单一认识。但是，近年来区块链发展迅速，随着网络结构、共识机制和激励机制的多样性发展，区块链去中心化特征和金融信用中介特征具有了更多的契合点，大大提高了区块链金融应用场景的可扩展性。

金融业作为实体经济的工具和媒介中枢，市场主体多元、业务种类繁多、交易流程各异，因此，金融业务的信息化管理模式也需要不断创新。美国区块链科学研究所创始人Melanie Swan认为，应该把区块链视为与互联网类似的事物，将其作为一种综合的信息技术，其中包含多层面的应用[13]。区块链的主要机制包括网络结构、共识机制和激励机制，每项都有多种选择，可以实现区块链的延展性应用，以适应多样化金融业务的管理要求。具体内容如下图所示。



基于区块链的金融交易基础架构图

由于区块链主要机制的可延展性，在裁剪和组合区块链主要应用特性的基础上，可以设计出适合不同金融业务的应用场景。下面列举几种可能的应用场景：

1. 法定数字货币发行。金融机构，尤其是中央银行，可以采用“公链式单链结构、权益证明机制、通证激励”的模式，在一国甚至全世界范围内发行法定数字货币。肇始于区块链激励机制的数字加密货币，已经表现出对国家货币主权的侵蚀和对法定货币秩序的冲击，随着区块链的发展，未来每个人都有可能成为信用中心和价值中心，理论上每个人都可以基于信用成为发币中心。鉴于目前的信用经济条件，中央银行需要将数字货币发行纳入统一监管体系[14]。目前，基于区块链发行法定数字货币，是很多中央银行开始考虑的问题。另外，中央银行还可以将区块链技术作为一种货币政策工具，更好地发挥宏观调控的作用。

2. 支付清算。商业银行可以采用“联盟链式单链结构、授权股权证明机制、手续费激励”的模式，建立全球范围的支付清算系统。依据商业银行的传统支付清算流程，完成一笔交易需要经过央行、开户行、代理行和对手行等多个环节，涉及多层信用担保，耗时长、成本高。基于区块链建立支付清算体系，充分发挥区块链去中心化和自信任的特点，可以实现价值的数字化传输，提高跨区域支付清算效率。区块链上支付清算信息的可追溯性，也为统计资金流向提供了便利，有利于解决交易纠纷并防范洗钱等违法行为的发生。

3. 证券交易系统。投资银行可以采用“联盟链+链下网络、授权股权证明机制、手续费+保证金激励”的模式，基于区块链技术建立证券交易系统。通过联盟链整合不同交易所和证券公司交易数据，通过链下网络处理高并发的证券交易。主链记录交易信息摘要，交易主体选举产生记账节点，通过授权股权证明机制降低区块的确认时间和成本，实现信息公开透明、交易可追溯，降低信息不对称，使投资决策更加高效。早在2015年，美国Overstock就基于区块链技术开发了去中心化股票交易系统——美第奇项目（Medici Project），并且获得了美国证券交易委员会（SEC）的批准。对于该项目，美国乔治城大学金融学教授James Angel认为，使用一个类似于区块链的公共总账来管理证券或其他资产的前景是非常令人兴奋的。

六、区块链金融应用需要注意的问题

区块链金融应用前景广阔，需要协调好区块链去中心化特征和传统金融的信用中介功能，这同时也会带来新的监管问题，需要在鼓励创新和防范风险之间做好权衡，解决好区块链金融发展中的问题。区块链的主要特征是交易规则和交易信息的公开性，与此同时，又具有交易主体匿名性的特点，即交易主体实际身份和区块链虚拟身份的非绑定性，隐私保护比较完备[15]，但也造成了金融监管的难题。

1. 区块链金融应用的监管问题。

（1）需要构建新的监管框架。随着区块链的发展，未来每个自然人理论上都可以成为信用中心，甚至是发币主体。这就要求我们必须在传统金融理论的基础上，构建新的监管框架，以开放的心态，平等地对待各类主体，适应新的金融生态，建立新的监管理论，构建多主体共同参与的监管体系。

（2）需要正视变化的监管基础。区块链技术和区块链信用经济的发展，深刻地改变着金融监管基础，引起了金融市场生产关系的微妙变化。例如，金融市场经济资源的分散化、参与主体的多样化、金融机构边界的模糊化、资源价值的虚拟化等。金融监管需要正视金融市场微观主体的新特点。

（3）需要构建科学的监管模式。随着区块链的发展，监管模式需要向智慧方向发展。培育自学习、自适应、自协调、自进化的监管模式，以适应基于区块链不断产生、发展、迭代的新型应用，在加强监管和鼓励创新之间做好权衡。

2. 区块链金融应用对传统金融机构的冲击。

（1）区块链的去中心化特点对传统金融体系中介功能的冲击。目前，传统金融体系大多建立在一对多的中心模式上，交易系统主要基于第三方信用。区块链发展带来的一个主要变化就是去中心化，通过内在的共识机制和激励机制，实现了交易信用和数据存储的去中心化，从而对传统金融体系中介功能造成了冲击。

（2）区块链的自治特点对传统金融体系信用功能的冲击。区块链点对点式网络架构、广播式的信息传输模式、交易信息和交易标的物的历史记录不可篡改性，都大大增强了金融交易行为和交易主体的自治性。理论上，独立的自然人都可以成为区块链上的信用主体和价值主体，因此随着区块链的发展，自然人也可以基于自身信用成为货币发行主体，这种发展趋势极大地削弱了传统金融体系的信用担保功能。

3. 区块链金融应用和客户隐私保护的矛盾。首先，区块链系统中的交易规则和交易信息是公开、透明的，并且无法篡改。但是，许多区块链具有交易附言功能，此功能下同样无法更改和删除信息，本文认为这是隐私保护的隐患。如果有人通过区块链交易附言功能暴露他人隐私或者散布谣言，该信息同样无法删除。其次，区块链的通证机制是以加密算法为基础，区块链交易终端的虚拟身份独立于交易主体的实际身份，交易主体只要建立虚拟身份就可以参与交易，各类区块链节点之间不存在公开身份的必要性，这就形成了区块链虚拟空间和物理空间的相对隔离，追踪用户真实身份的难度很大。最后，区块链交易信息公开和交易主体匿名的特点带来的挑战是多方面的：一是交易主体的匿名性，使相关机构对洗钱等违法活动难以取证和监管；二是跨境资本的非正常流动难以监管；三是为行贿、受贿等违法犯罪活动提供了可选的途径。

七、总结

区块链的发展是信息技术应用的自然延伸，带来了信息传输性质的突破性变化。在这个过程中，区块链所体现出来的技术特征使其在金融行业具有很大的应用空间。因为比特币和以太坊等区块链系统的影响广泛，目前较多的研究集中在公链式区块链的应用上。又由于ICO和算力竞赛中的过度投机行为，使很多人对区块链的发展产生了一定程度的误解。但是，区块链作为计算科学和机制设计的结合，在信息管理领域不断创新，应用空间也在不断扩展。

相对于区块链的技术架构，其机制设计逐渐表现出强大的吸引力。肇始于比特币系统的诸多机制设计，在短短的十年内又有了很大的发展。侧链和链下网络的提出，突破了原有区块链数据处理容量的瓶颈，使得区块链在金融领域的应用具备了可延展性。共识机制的不同尝试，大大改变了我们对区块链交易确认时间长和成本高的固有印象。激励机制的不断发展，也产生了类似手续费激励、保证金激励等更适合金融业务的区块链激励模式。在裁剪、组合、发展区块链技术优势的基础上，区块链的金融应用前景将会越来越广阔。

主要参考文献：

[1] Nakamoto S.. Bitcoin：A peer－to－peer electronic cash system[EB/OL]. http://www.bitcoin.org/bitcoin.pdf，2016－11－28.

[2] Heires，Katherine. The risks and rewards of blockchain technology[J]. Risk Management，2016(2)：4～7.

[3] 袁勇，倪晓春，曾帅，王飞跃. 区块链共识算法的发展现状与展望[J]. 自动化学报，2018(11)：2011～2022.

[4] 曹淑艳，王小钰，卢艳桥，曹亚南. 中外区块链研究综述[J]. 理论学习与探索，2017(3)：84～87.

[5] 卿苏德，姜莹，王秋野. 区块链的技术原理和意义[J]. 电信网技术，2016(12)：14～20.

[6] Decker C.，Wattenhofer R.. Information propagation in the Bitcoin network[C]. IEEE Thirteenth International Conference on Peer－to－Peer Computing，2013：1～10.

[7] 邵奇峰，金澈清，张召，钱卫宁，周傲英. 区块链技术：架构及进展[J]. 计算机学报，2018(5)：969～988.

[8] 姚忠将，葛敬国. 关于区块链原理及应用的综述[J]. 科研信息化技术与应用，2017(2)：3～17.

[9] Back A.，Corallo M.，Dashjr L.，et al.. Enabling blockchain innovations with pegged sidechains[EB/OL]. http: //www. opensciencereview. com/papers/123/enablingblockchain－innovations－with－pegged－sidechains，2014－10－22.

[10] Eisenberg E.，Gale D.. Consensus of subjective probabilities：The pari－mutuel method[J]. The Annals of Mathematical Statistics，1959(1)：165～1168.

[11] 袁勇，王飞跃. 区块链技术发展现状与展望[J]. 自动化学报，2016(4)：481～494.

[12] Vukolic M.. Rethinking permissioned blockchains[A]. ACM Workshop on Blockchain，Cryptocurrencies and Contracts[C]. New York：ACM Press，2017：3～7.

[13] 长铁，韩锋等. 区块链：从数字货币到信用社会[M]. 北京：中信出版社，2016：181～182.

[14] 杜金富. 数字货币发行理论与路径选择[J]. 中国金融，2018(13)：34～36.

[15] 宫晓林，杨望，曲双石. 区块链的技术原理及其在金融领域的应用[J]. 国际金融，2017(2)：46～54.

作者单位：北京邮电大学经济管理学院，北京100876