財經法學 No. 3，2019
pp. 66 - 78

区块链下证券结算的变革、应用与法律回应

卜学民*

内容提要：区块链技术作为最新科技的代表，应用于证券结算领域可以实现证券的直接所有权、自动同步数据、自动灵活结算，并增强安全性，弥补传统证券结算中效率低、成本高、安全性差的缺陷。目前的三种主流应用模式中，核心机构共享模式能够克服各自为政模式和完全无中介模式的缺陷，既实现效率、成本和安全价值，又可以匹配传统的证券结算，具有很强的应用价值。应用核心机构共享模式，必须在法律上实施嵌入式监管、对智能合约进行多角度的管理、将六次验证完成时间作为结算最终性的时点，并且明确区块链技术下证券结算的法律责任。

关键词：区块链　结算变革　应用模式　智能合约　嵌入式监管

区块链技术是继互联网之后人类历史上出现的一项颠覆式创新技术，被认为是“最有可能改变未来十年商业模式的技术”，[1]能极大地提高社会生产率、降低生产成本、促进交易安全。区块链技术的应用前景也十分广阔。目前，世界主要国家和主要机构正在积极探索和推动区块链技术在证券、银行、保险、电子商务、公共服务等领域的应用，以提高本国产业的国际竞争力。为了促进“中国梦”的早日实现，我国也应当把握住区块链技术所带来的历史性发展机遇。事实上，中国政府非常重视区块链技术的研究和应用。国务院发布的《“十三五”国家信息化规划》就明确将区块链作为一项重点前沿技术，提出需加强区块链等新技术的创新、试验和应用，以实现抢占新一代信息技术主导权。对于证券市场而言，区块链技术能够以其去中心化、数据共享和不可篡改的特征优化证券交易的结算，具有明显的效率、成本和安全性价值，将其应用于证券市场已经是大势所趋，但必须在应用模式上加以探索，在提高效率和降低成本的同时，要

* 卜学民，对外经济贸易大学法学院博士研究生。

〔1〕 See Don Tapscott, Alex Tapscott, The Impact of the Blockchain Goes Beyond Financial Services, HARV. BUS. REV., May 10, 2016, available at https://hbr.org/2016/05/the-impact-of-the-blockchain-goes-beyond-financial-services, last visited on Mar. 13, 2019.

尤其重视证券市场风险的控制，设计出适合证券结算的最佳模式，识别新技术应用带来的新的法律挑战并予以积极应对。因此，本文集中研究区块链给证券交易带来的变革、应用及法律应做出的回应。

一、区块链技术对传统证券结算的变革

目前我国证券结算主要由中央国债登记结算有限责任公司（“中债登”）和中国证券登记结算有限公司（“中证登”）负责，其职责主要包括证券登记、结算和账户维护三个方面。此外，与证券相关的如权益派发、托管、融资、报告和证券借贷等服务也属于其职能范围。在履行职责过程中，他们需要与交易所和结算参与人（一般是证券公司）合作，保管所有交易数据、进行数据更正和维护，交易成本甚巨、工作效率较低并且安全性较差。区块链具有去中心化、数据共享、不可篡改等特征，恰好可以弥补传统证券结算的不足。

（一）传统证券结算体系的痛点

目前我国证券结算过程以结算公司作为中央枢纽，结算公司与交易所、银行和证券公司之间相互配合，共同完成结算行为。我国证券结算的流程如图1所示，其具有以下缺陷：第一，成本高昂、效率低下。证券的结算需要证券公司、证券交易所、结算公司、银行等金融机构的参与，流程冗长而且复杂，在二级结算的架构下，证券经纪商还需要交纳抵押品来降低因违约而给中央对手方造成的损失，这既增加了交易抵押品的数量，又降低了资金和证券的流动性，在2013年环球同业银行金融电讯协会（SWIFT）的结算中，托管和抵押品管理收入达到了400—450亿美元，约占总交易价值链的13%。其中约30亿美元交给中央证券保管局，另有约390亿美元给托管人。〔2〕投资者需要有偿委托证券公司在金融机构进行交易结算，每个参与的金融机构也都有自己的交易分类账，这会导致分类账之间并不实时一致，需要不同机构之间进行对账并予以人工调整。全球每年的核心交易后流程、参考数据、对账、交易费用管理、客户生命周期管理、协同行为、税务和监管报告方面的花费为170亿至240亿美元。部分是由于中介机构对于每个交易都使用自己的系统来处理交易、发送和接收指令、进行数据协调和错误管理等，链条中的每个中介需要保持交易记录的更新。〔3〕加上用于了解客户（KYC）和反洗钱（AML）合规费用，资本市场中台和后台每年的成本超过1 000亿美元。〔4〕成本巨大并且效率低下的事实已经不言自明。第二，安全性低。首先，结算数据保存在中心化的金融机构处，一旦受到攻击会导致数据被盗或者账户的券款与实际不符，造成安全威胁。其次，为应对交易对手风险，中央对手方（CCP）一直要求买卖双方提供抵押品，并承担重置成本风险和流动性风险，一旦发生交收违约，中央对手方便会动用抵押品，这也从一个侧面说明了交易风险

〔2〕 See Oliver Wyman, Swift, The Capital markets Industry: The Time They Are A-chang-in , 8 (2014), available at https://www.oliverwyman.com/content/dam/oliver-wyman/global/en/files/insights/financial-services/2014/September/the-capital-markets-industry.pdf, last visited on Jan. 6, 2019.

〔3〕 See Broadridge, Charting a Path to a Post-Trade Utility, Broadridge White Paper, 4 (2015).

〔4〕 See Mainelli M. and Milne A., The Impact and potential of blockchain on the securities transaction lifecycle, SWIFT Institute Working Paper, No. 2015-007, 8 (2016).

的存在。另外，由于缺乏透明度，目前市场上还存在着大量的内幕交易行为和裸卖空〔5〕等欺诈行为，对金融安全和稳定造成了巨大威胁。

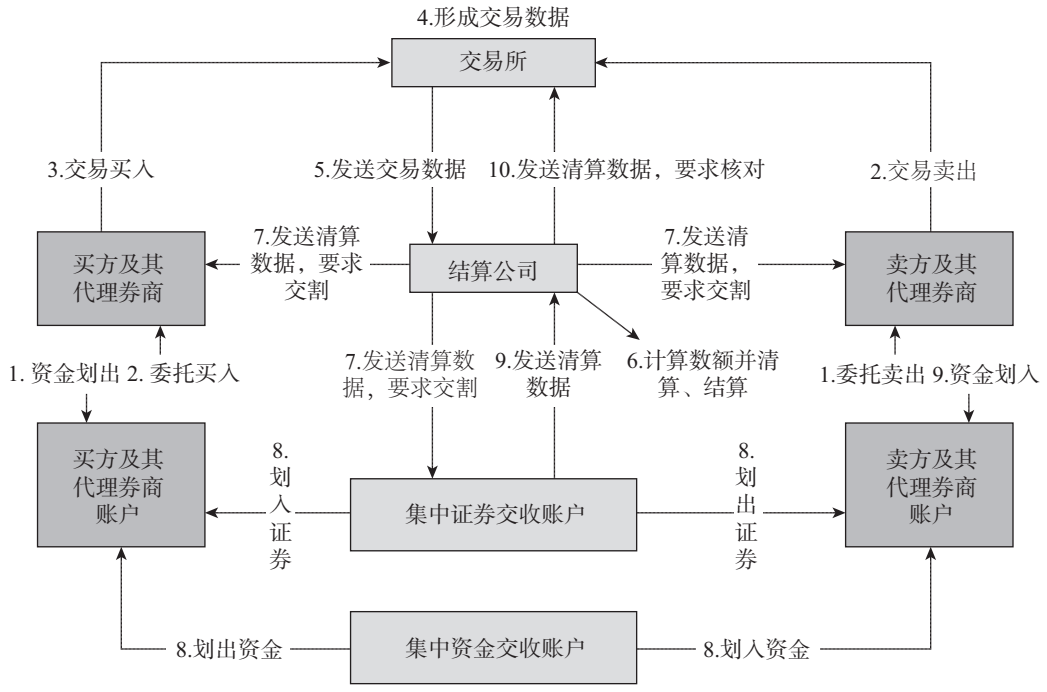

图 1　我国证券交易结算流程

造成传统结算存在缺陷的原因是多样的，第一，历史上，证券的存在形式一直是纸质的，因而需要中心化的受信机构存在来发行、保管、清算和交收，即使在无纸化改革后，仍然存在中心机构，证券账户与投资者、证券公司以及证券登记结算机构之间仍然存在着复杂的法律关系。〔6〕第二，出于证券结算的专业性和复杂性、纸质证券需要被固定以便通过账面转账进行交易和减少证券交易直接参与主体的考虑，各国法律普遍规定证券的持有、交易和结算必须通过证券经纪商进行，使得间接所有权取代了直接所有权，这增加了代理和协调成本并影响了效率。第三，结算行业一直以来存在绝对的进入壁垒，这使结算公司处于垄断地位，没有压力和动力去研发新技术，而现有技术无法使结算在所有金融机构之间具有相互操作性，因而，这些问题一直存在于结算行业而没有得到解决。区块链技术的出现几乎能够克服所有障碍来解决证券结算缺陷，因此具有巨大的应用潜力。

〔5〕 裸卖空是指既不拥有也未借入股票的市场参与者卖出股票（多头或空头），股票下跌时再买回以获取高额利润的行为。在 2008 年金融危机发生时发现了大量的裸卖空行为，这既是金融危机发生的一个诱因，也导致金融危机的破坏性逐渐加深。See Gary J. Aguirre, Blockchain for security: black swan or in-house pet? p. 4 - 5, 22 No. 1 Wallstreetlawyer. com: Sec. Elec. Age NL 1。实质上，它是假冒股票的销售。裸卖空可能是导致贝尔斯登、雷曼兄弟崩盘和摩根士丹利近乎崩盘的一个因素。See Bill Saporito, Are Short Sellers to Blame for the Financial Crisis? Time Magazine, Sept. 18, 2008, available at http://www. time. com/time/business/article/0, 8599, 1842499, 00. html, last visited on Feb. 6, 2019.

〔6〕 参见叶林：《无纸化证券的权利结构》，载《社会科学》2009 年第 3 期。

（二）区块链技术对传统证券结算的优化

将区块链技术应用于证券结算领域具有相当大的可行性与必要性：第一，每个结算参与方都拥有相同的分类账副本，可以通过节点在点对点的基础上连接起来直接进行交易和结算。第二，区块链技术允许结算参与方在其中拥有不同的权限并发挥不同的作用，例如，某些参与者只被允许作为发送和接收现有资产的资产转移节点，其他参与者被许可发行新资产、验证交易、将交易历史更新到分类账或仅限于阅读分类账。〔7〕第三，资产的所有权可以存储在区块链的分类账中，能够显示所有交易历史和当前所有权状态，证券的所有交易历史和权利归属都有据可查。第四，区块链技术协议可定义资产转移过程所需的程序，并依靠智能合约〔8〕技术自动执行交易，省去了结算过程并保证了交易的执行。第五，区块链技术结算系统意味着金融机构可以共享同一种证券资产的数据，并对不在其原有的私有数据库内的证券的执行、清算和结算进行持续追踪，且不需要任何中央数据管理系统的介入，可以同时实现安全和效率价值，且保证了监管合规性。〔9〕

与传统的结算系统相比，区块链技术下的证券结算系统的不同，参见表1。

表1　　传统结算系统与区块链技术结算系统的比较

不同点	传统结算系统	区块链技术结算系统
数据存储方式	集中式，存储于各金融中介系统	分布式，多份副本存储于结算参与方
数据一致性	各自保存自有数据，后台调整	数据同时更新，自动保持一致
交易机制	经纪制	直接交易
结算机制	中央对手方	智能合约
结算周期	T＋1；T＋2	近乎实时结算
数据管理	独立的数据库管理系统	由有权限的节点维护，不可篡改
透明度	仅特定机构可见部分交易记录	可追溯券款历史记录

区块链技术以其去中心化、数据加密共享、公开透明、可追溯并不可篡改的特征，并辅之以智能合约技术能够有效弥补目前证券结算领域的不足。在区块链技术下的所有结算系统中，依靠共识协议和智能合约，交易处理分两步完成：1. 交易有效性，即它是否满足签名核对、交易规则、证券和资金的合法所有权等一系列必要的条件；2. 交易唯一性，即通过确保交易中包含的

〔7〕 See Mills, David, Kathy Wang, Brendan Malone, Anjana Ravi, Jeff Marquardt, ClintonChen, Anton Badev, Timothy Brezinski, Linda Fahy, Kimberley Liao, Vanessa Kar-genian, Max Ellithorpe, Wendy Ng, and Maria Baird , Distributed ledgertechnology in payments, clearing, and settlement, Finance and Economics Discussion Series 2016－095, Washington: Board of Governors of the Federal Reserve System, 12 (2016).

〔8〕 智能合约是一套以数字形式定义的承诺，包括合约参与方可以在上面执行这些承诺的协议，其语言是计算机语言中的代码，而不是传统合同中的文字，也不是法律语言。智能合约的执行条件必须客观明确，不需要经过解释。See Nick Szabo, The Idea of Smart Contracts (1997), available at http://szabo.best.vwh.net/smart_contracts_idea.html; Josh Stark, last visited on Feb. 12, 2019. Stark认为智能合约有两种内涵。一是“智能合约代码”，指软件在实际操作中能够代理执行某些义务，在共享总账中拥有某些资产的控制权。二是“智能法律合约”，指解释法律合约在软件中如何表达和执行。See Stark J, How close are smart contracts to impacting real-world law, available at https://www.coindesk.com/blockchain-smarts-contracts-real-world-law, last visited on Feb. 12, 2019. 关于智能合约更加详细的讨论，See Kevin Werbach, Nico Cornell, Contracts Ex Machina, 65 *DUKE L. J.*, 313－381 (2017).

〔9〕 See Pinna A., Ruttenberg W., Distributed Ledger Technologies in securities post-trading, ECB Occasional Paper, Series no. 172, 3 (2016).

现金和证券与任何其他未决交易无关来确认交易以避免双重支付问题。区块链技术的应用，使证券交易结算能够在很少甚至没有中间机构的情况下，实现结算参与主体在既有证券规则框架下，用自有资金和合法拥有的证券进行交易结算，防止了裸卖空和一券多卖等违法行为的发生，提升了证券结算的效率、降低了成本，并且能够保障交易的高全性，这主要表现在以下方面：

第一，投资者拥有证券的直接所有权。在目前的证券市场中，大多投资者不是其证券的直接所有者，而是通过证券代理商等金融机构持有证券。在证券代理商存在擅自买卖、违法买卖证券和其他违规操作的情况下，这种证券的间接持有制会带来法律和操作风险，使投资者处于证券交易结算链条中最不利的地位，〔10〕从而导致投资者的重大损失。而区块链技术可以实现投资者的直接所有权，降低投资者的法律风险和中介成本，并提高后台效率。证券的直接所有权还可以提高证券的透明度，因为投资者可以直接控制其持有的股份，发行人可以直接追踪证券所有者。

第二，降低数据管理成本和协调成本。区块链技术能够自动更新交易和结算数据，所有证券参与主体拥有的分类账具有同一性，这可以减少结算参与主体协调的需求，并且，各结算参与主体的分类账的同一性特点使得集中维护结算数据失去必要，这些变化都可以带来成本的降低和效率的提升。根据估计，区块链技术将能减少 50％甚至更多的金融证券交易成本。〔11〕

第三，自动清算并结算。在区块链技术下的证券结算系统中，一旦两个交易对手之间达成交易，不需要进一步确认或对账，因为所有相关信息已经在参与者之间共享。区块链下证券交易的结算是通过自动执行区块链中智能合约的方式完成的，交易的结算更加快捷。证券交易智能合约达成并经由特定的共识机制形成区块后，合约便不可更改、不可撤销，并在智能合约设定的交易条件全部满足后，自动执行，嵌入智能合约的资金、数字资产等交易标的同时转向对方账户，实现自动结算。

第四，灵活的结算时间。区块链技术可以缩短证券交易的结算周期。目前我国的证券多运用中央对手方实行多边净额结算，A 股和 B 股实行 T＋1 的交割方式，实行回转交易的证券遵循 T＋0的交割方式。T＋1 交割的情形下，参与者至少有一整个工作日准备结算并在必要时借入证券或现金。T＋0 的周期需要在交易之前预先储备现金或证券，这将对流动性管理产生影响。当前的结算周期不长并不是由于技术限制，而是由于后台管理流程、法律安排和流动性管理实践。区块链技术可以实现投资者之间的点对点直接交易，无须中央对手方充当买方的卖方和卖方的买方，无须事先储备或借入资金和证券，因而，区块链技术可以缩短结算周期。并且，区块链技术还可以实现的证券结算的 T＋N，允许用户设定任意的交易周期来获得流动性。〔12〕这种结算方式可以实现近乎实时的结算，并极具灵活性。

第五，安全性增强。首先，区块链技术降低了证券交易的违约风险。为了提升效率和降低风险，我国现行证券交易的结算采用多边净额结算制度，中央对手方承担着对手方违约的风险。而

〔10〕 See Micheler E., Custody Chains And Asset Values: Why Crypto-Securities Are Worth Contemplating, 74 (3) *Cambridge Law Journal*, 533 (2015).

〔11〕 参见前引〔4〕，Mainelli M. and Milne A. 文，第 8 页。

〔12〕 See Morgan Stanley, Blockchain in Banking: Disruptive threat or tool, Morgan Stanley Global Insight, 7 (2016).

区块链能够实现即时货银对付，证券交收和资金交收被包含在一个不可分割的操作指令中，交易同时成功或失败，实现货银对付并降低因一方违约而造成另一方受损的风险。违约风险的减少，也会降低其他风险出现的可能，〔13〕比如杜绝幌骗和裸卖空等非法证券行为。因为交易者必须真正拥有加密证券之后，才能形成私钥、公钥从而顺利完成交易，在区块链加密证券交易系统中，如果一项交易没有彻底达成，是不可能出现在区块链这个公共账本上的。〔14〕其次，区块链上的每一次交易都会形成相应的无法篡改的时间戳，且可以追溯到所有的资金和证券流向。这可以提高交易的透明度，也为监管带来便利，增强了交易安全。最后，区块链上的每个参与节点都备份了已经发生的所有交易，使系统对恶意攻击行为更有弹性，在发生此类攻击时更快地恢复交易数据。并且，使用加密签名来访问数据和加密分类账的元素，也将增强其安全性。此外，区块链技术还能够方便监管，如前所述，区块链技术可以获得具有同一性的交易数据，并能够追溯任何资金或证券流的历史。在将监管机构设置为区块链中的一个中心节点后，监管机构可以读取和访问交易结算分类账，这将提高监管的有效性并降低报告成本。

二、区块链技术应用于证券结算的模式及选择

（一）模式类型

区块链技术被认为是一种具有重大影响的根本性创新和能够影响整个证券交易链的系统性创新，可以使证券结算的规则、制度和过程发生重大而全面的变革，并可能破坏当前市场现有主体在证券结算中的地位。比如，在区块链技术应用于证券结算的最激进方案中，交易的结算仅发生在最终买方和卖方之间，不再需要结算公司，而是存在促进双边结算的技术方案提供商。目前来讲，在证券结算行业应用区块链技术主要有以下三种模式可供选择。

1.“各自为政”模式

该模式是指证券结算的参与机构各自开发符合自身需要的区块链技术应用系统，来提高内部效率，但是，机构之间并不寻求联系为一个有机的整体，各自的系统缺乏协作性，不同机构的数据也缺乏自动更新的一致性，仍然各自保存着自己的交易结算数据。此模式下的结算流程与传统的结算流程相比，几乎没有什么不同，区块链技术仅仅是对于机构本身具有直接的效率、成本和安全价值。参见图 2。

2.“核心机构共享”模式

“核心机构共享”模式是指以传统的证券交易框架为基础，将核心机构纳入证券结算数据的共享范畴，核心机构之间彼此互联互通，实现数据的同步更新，并保持一致性。而核心机构之外的其他传统结算参与中介机构则并不加入相同的区块链结算系统，并且根据需要来确定其是否有继续发挥作用的必要。证券的个人投资者也不加入区块链系统。参见图 3。

〔13〕 参见刘瑜恒、周沙骑：《证券区块链的应用探索、问题挑战与监管对策》，载《金融监管研究》2017 年第 4 期。

〔14〕 参见万国华、孙婷：《“区块链＋证券”的理想、现实与监管对策研究》，载《上海金融》2017 第 6 期。

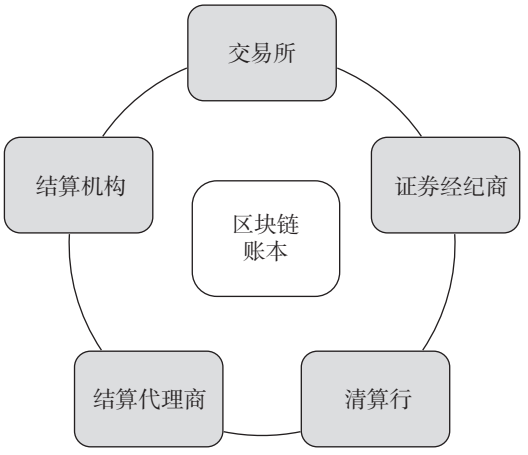

图 2　“各自为政”模式

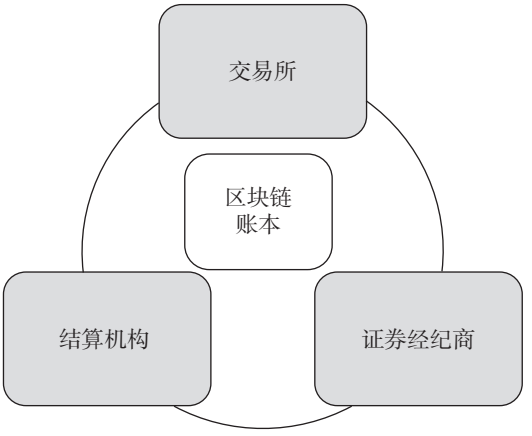

图 3　“核心机构共享”模式

3.“完全无中介”模式

“完全无中介”模式是指在证券发行和交易以及结算链上，仅存在证券交易所、发行人和证券投资者三类必备主体。在这种应用模式下，发行者在区块链上发行证券后，投资者在证券交易所的组织下进行证券交易的同时实现了证券的自动化结算，也就是说，证券的自动结算将完全取代传统的结算流程。参见图 4。

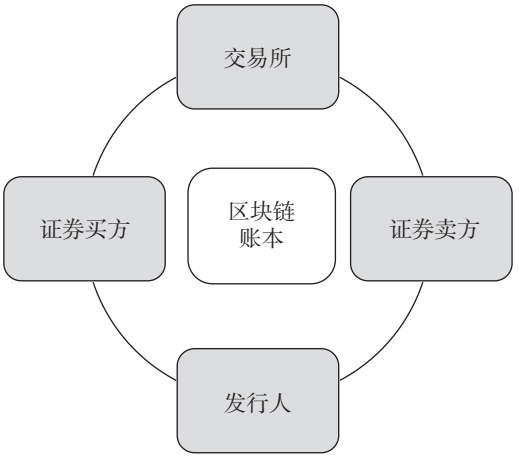

图 4　“完全无中介”模式

（二）模式选择

以上三种模式构成了目前将区块链技术应用于证券结算领域的主流方案，各自对现有证券结算模式的变革程度不同，需要监管和法律政策的调整也不同。不同的应用模式也有着各自不同的考量，就区块链技术的革命性和模式涉及的主体数量而言，“各自为政”模式下的证券结算变革程度是轻微的。与传统的证券结算相比，所涉及的机构并没有不同，所有机构依旧使用并保存各自的数据库，机构之间对账的需求依然存在，结算过程的中间人链条也没有变化。〔15〕但有两点进步之处：一是作为结算的某一环节的机构内部效率提高了，成本亦随之降低；二是证券所有权

〔15〕 参见前引〔9〕，Pinna A.，Ruttenberg W. 文，第 29 页。

的变动将接近实时更新。但是，该模式所提高的效率和降低的成本仅存在于机构内部，对整个证券市场而言是间接的，投资者能获益之处在于机构服务成本降低而带来的服务费用的减少。就该技术所能对整个证券市场带来的变革而言，并没有将区块链技术的优势全部发挥出来，而只是一种十分低层次的应用，可以说是“大材小用”。因而，其只是当下区块链技术未能广泛应用情况下，各机构内部开发应用区块链技术的一种初级阶段，而绝非未来区块链技术在证券结算领域大规模应用的最佳选择。

“完全无中介”模式可以推进投资者直接参与证券的交易，将在更大范围推动证券市场的开放化，证券发行方和买卖双方直接接触进行证券交易，整个中间环节都将被省略，而智能合约将自动执行任何证券交易，实现实时结算。这种模式的优点在于完全省去了传统结算的中间链条，证券直接所有权节省了投资成本、保障了投资者权利，自动结算省去了托管和结算费用，并降低了交易对手方风险，最大程度地简化了交易流程，实现了证券交易的高效、便捷、低成本。但是这种模式的缺点也是显而易见的，首先，此种模式的最大阻碍会是最大化“知晓客户”和反洗钱的难度，〔16〕若允许投资者直接以匿名的方式进入区块链进行证券交易并实时结算，将很难追踪到其真实身份，会为不法分子以投资之名行反洗钱之实打开方便之门。其次，目前的交易验证技术不能充分保护隐私，区块链上的账本对所有投资者开放，会使别有用心的投资者通过追踪普通投资竞争对手的交易活动获取这些竞争者的流动性交易需求，寻求不公平的交易。再次，此种模式下，证券公司的证券经纪业务和结算公司的结算业务将面临被取代的危机，尤其是后者，作为证券市场的主要基础设施之一，短时间内技术无法做到全面取代其所有的结算职能，尤其是涉及在结算过程中需要做出主观判断的职能。最后，部分中小投资者依赖于证券经纪商和结算公司提供的专业服务，若由其自主进行所有的证券交易和结算行为，对于他们来说是一项不小的挑战。只有存在以下三个条件，才能实现区块链技术跨市场、跨流程、跨资产类别的长期大规模采用：（1）极其强大的技术产品；（2）对技术解决方案有着深刻的熟悉和信心；（3）大量市场参与者对时间和资源进行大量投资。〔17〕而目前三个条件都不具备，故短时间内很难采用第三种模式。

“核心机构共享”模式则克服了以上两种模式的缺陷，具有应用前景。第一，分布式账本将使得现有的证券结算市场更快、更自动化，证券交易将由同一个分布式账本来服务和结算，而不是使用各方的私藏数据库，并且在全行业应用该模式的情况下，证券账户将会得到自动更新。第二，区块链技术从根本上重塑了结算结构，但完全脱媒似乎不太可能。在智能合约技术完全成熟并应用后，核心机构之外的托管人变得冗余，因中央对手方原有的大部分功能已经通过智能合约技术实现了自动化，其大部分职能也将被取代。但是，一方面，成本、风险和技术专业知识要求的障碍可能会阻碍最终投资者操作自己的分类账。他们很可能依赖于分类账服务提供商。另一方面，结算机构的部分职能仍需继续存续，因为衍生品交易和现货交易在执行和结算之间仍有延迟

〔16〕 参见徐忠、邹传伟：《区块链能做什么、不能做什么?》，中国人民银行工作论文，No. 2018/4。

〔17〕 See Oliver Wyman, Blockchain in Capital Markets, The Prize and the Journey, 15 (2016), available at http://www.euroclear.com/content/dam/euroclear/Marketing/Brochures/BlockchainInCapitalMarkets-%20ThePrizeAndTheJourney.pdf, last visited on Feb. 10, 2019.

的可能，依然需要 CCP 的清算，〔18〕CCP 的重置成本保证或默认管理功能等需要自由裁量或判断的功能，也不太可能通过区块链技术实现。〔19〕违约判定、拍卖成功判定等特殊情形的处理需要自由裁量权。〔20〕该模式取消了一些中介机构或者中介机构的职能，但保留了核心机构，使其仍可以发挥原有不可取代的职能，继续作为证券和现金账户之间的桥梁，易于在机构存废之间做出平衡，并且提高了效率、降低了成本。第三，对于监管者而言，由于证券交易和结算信息已经被导入交易信息库，区块链技术下的交易结算信息将实时更新，证券交易结算的报告会自动、近乎实时地生成，场外执行的证券交易（OTC）也会变得更透明，监管者可以对每一笔交易和未偿持仓进行追踪。〔21〕只要监管者有权限访问区块链账本，监管信息就会完全对称，也就可以进行实时而有效的监管。因此，从穷尽技术价值和可行性的角度来说，此种模式是更值得采用的模式。

三、区块链技术应用于证券结算的法律挑战及应对

新技术会使现有的法律制度面临日益频繁的“破窗性”挑战和“创造性”破坏。〔22〕每一次技术的重大突破都会对法律规则和制度形成冲击，为应对技术带来的挑战，必须能够识别这些挑战，并在法律上予以回应。美国特拉华州、〔23〕亚利桑那州〔24〕等已经颁布了相应的立法，在区块链立法上迈出了重要一步。我国虽然在 2019 年通过了《区块链信息服务管理规定》来规范区块链技术的应用，但是无论从法律位阶还是内容上都远未达到全面规范区块链技术的程度。对于证券市场而言，法律在监管方式、对智能合约的管理、结算最终性以及法律责任上并无明确规定，这会成为区块链技术在这一领域的重大挑战，必须做出回应。

（一）监管缺失：嵌入式监管

尽管区块链技术以去中心化为核心特征，但是并不意味着区块链就没有中心。区块链实际上包含公有链、联盟链和专有链三种类型。〔25〕公有链对所有人开放，联盟链只对经行业联盟许可的主体开放，而专有链仅对特定机构内部开放。对于证券等金融行业而言，因涉及数据和隐私的

〔18〕 See ESMA, The Distributed Ledger Technology Applied to Securities Markets, ESMA Report, 21 (2017).

〔19〕 See Mark Manning, Maxwell Sutton and Justin Zhu, Distributed Ledger Technology in Securities Clearing and Settlement: Some Issues, 3 *JASSA The Finsia Journal of Applied Finance*, 30, 31 (2016).

〔20〕 参见《上海清算所中央对手方清算业务金融市场基础设施原则信息披露》原则要点 13.2，该要点规定：FMI 应为实施违约规则和程序做好充分准备，包括规定适当的自主裁量程序。

〔21〕 参见前引〔9〕，Pinna A., Ruttenberg W. 文，第 8 页。

〔22〕 参见马长山：《智能互联网时代的法律变革》，载《法学研究》2018 年第 4 期。

〔23〕 特拉华州 SN183 项法案第 6、25、26、27 节分别修改了原《公司法》的 18—104（g）、18—302（d）、18—305（d）和 18—404（d），明确允许国内有限责任公司运用包括分布式记账技术在内的电子数据库网络进行公司账目创建、保存和记录的电子传输。See Bill Text DE S. B. 183, Delaware Second Year of the 149th General Assembly, section 6/section25 - 27 (2017).

〔24〕 亚利桑那州通过的《区块链法案》，规定了区块链和智能合同的使用规范，同时声明所有与区块链相关的数据都“被认为是电子格式并成为电子记录”，予以认可。See Act of Mar. 29, 2017, Ariz. Rev. Stat. § 44 - 7003ch. 97, Ariz. Sess. Laws (2017).

〔25〕 根据 2016 年 10 月工信部信息化和软件服务业务司发布的《中国区块链技术应用和发展白皮书》：公有链的各个节点可以自由加入和退出网络，并参加链上数据的读写，运行时以扁平的拓扑结构互联互通，网络中不存在任何中心化的服务端节点；联盟链的各个节点通常有与之对应的实体机构组织，通过授权后才能加入与退出网络，各机构组织组成利益相关的联盟，共同维护区块链的健康运转；专有链的各个节点的写入权限收归内部控制，而读取权限可视需求有选择性地对外开放，专有链仍然具备区块链多节点运行的通用结构，适用于特定机构的内部数据管理与审计。

保护，存在一个或者多个中心的许可链更适合在该行业应用。〔26〕更重要的是，证券等金融行业的安全与稳定至关重要，没有监管的证券业是不可思议和不能接受的。完全去中心意味着匿名交易下的监管缺失，容易成为内幕交易和洗钱等金融犯罪的保护伞。此外，证券交易要实行实名制，没有中心的公有链无法对数据访问进行控制，会造成商业秘密和隐私的泄露。〔27〕况且，区块链的运行需要一定的主体进行维护，并在区块链下证券交易的资格准入、权限授予等方面发挥重要作用，保证区块链证券交易的高效安全，而维护和管理者本身也就是一个中心。另外，一旦采用公有链，原始开发团队就失去了控制权，很难修改区块链运行规则，故而风险性极高。

将区块链应用于证券交易领域，要以去中心化为基础，但是完全去中心化又不现实，无法解决区块链的运行和证券交易市场监管问题，因此有必要辅之以一定的中心机构或说是弱化的中心机构，这才是当前证券市场应用区块链技术的最佳选择。对于监管者而言，需要以嵌入式监管的方式进行监管，主要包括：第一，在证券结算行业应用区块链技术应该应用平衡“中心化”和“去中心化”优缺点的联盟链，〔28〕限制应用专有链，禁止应用公有链。〔29〕因为公有链对所有人开放，没有中心，容易导致区块链系统失控，进而破坏证券结算市场的稳定性。专有链仅存一个中心，无法适应证券结算领域诸多监管主体的需要，也容易形成对证券结算的绝对控制，安全性较低。〔30〕联盟链则存在多个中心，其运行由多个中心共同决定，一方面可以满足监管层作为区块链上的中心节点以进行监管需要，另一方面有助于将证券结算中的核心参与机构作为主要验证节点和自律监管节点，以防止恶意欺诈验证，造成交易损失。第二，证监会等国家机关应作为一级中心节点嵌入区块链，证券交易所作为二级中心节点嵌入区块链。将监管层的核心机构设置为中心节点，不仅能够增强其获取信息的及时性和有效性，便利监管，而且能够使其在发生紧急情况时采取停牌和停市等措施，维护证券市场的稳定。第三，规定监管机构有义务建设集中统一、信息共享的中央监管信息平台和中央监控系统，加强跨市场联动交易管理，强化信息采集和分析研判，实现跨市场交易行为的统一识别和监控，提升监管的及时性与有效性。〔31〕这也有利于监管层加强监管协作，全面、全程监测区块链上跨行业或跨市场交易可能出现的风险。〔32〕

（二）尚无法律规定规范智能合约：多维管理

智能合约是区块链 2.0 阶段的核心特征，想实现证券的自动实时结算，就必须同时应用智能

〔26〕 参见姚前、汤莹玮：《关于央行法定数字货币的若干思考》，载《金融研究》2017 年第 7 期。

〔27〕 参见前引〔26〕，姚前、汤莹玮文。

〔28〕 参见牛壮：《区块链对境内证券业影响分析》，载 http：//www. sse. com. cn/aboutus/research/report/c/4215082. pdf，最后访问时间：2019 年 3 月 3 日。

〔29〕 区块链包含公有链、联盟链和专有链三种类型。根据 2016 年 10 月工信部信息化和软件服务业务司发布的《中国区块链技术应用和发展白皮书》：公有链的各个节点可以自由加入和退出网络，并参加链上数据的读写，运行时以扁平的拓扑结构互联互通，网络中不存在任何中心化的服务端节点；联盟链的各个节点通常有与之对应的实体机构组织，通过授权后才能加入与退出网络，各机构组织组成利益相关的联盟，共同维护区块链的健康运转；专有链的各个节点的写入权限收归内部控制，而读取权限可视需求有选择性地对外开放，专有链仍然具备区块链多节点运行的通用结构，适用于特定机构的内部数据管理与审计。由于联盟链和专有链存在中心，也被称为“准区块链”。参见赵磊：《区块链如何监管：应用场景与技术标准》，载《中国法律评论》2018 年第 6 期。

〔30〕 参见任春伟、孟庆江：《区块链与证券清算结算》，载《中国金融》2017 年第 5 期。

〔31〕 参见前引〔30〕，任春伟，孟庆江文。

〔32〕 参见前引〔13〕，刘瑜恒、周沙骑文。

合约技术。与传统合约相比，智能合约表现出以下不同：第一，智能合约达成后，在满足执行条件后会自动成交和自动执行；第二，区块链技术具有不可撤销的特点；第三，智能合约的语言是计算机语言中的代码，而不是传统合同中的文字，更不是法律语言，也就是说，在最基本的合同中，对存在细微差别的法律的编码也会是巨大的挑战；〔33〕第四，智能合约执行的前提是执行条件必须客观明确，不需要经过解释，而传统合约的相关条件在不明确时可经解释加以确定；第五，智能合约的违约依赖于嵌入智能合约的保证金、数字财产等抵押品，而传统的合约依赖于通过法律手段维权。另外，智能合约在消耗成本、执行效率方面也有所不同。这些不同改变了证券交易行为的模式，也需要法律明确对智能合约的管理，主要包括：(1) 关于智能合约的性质，智能合约自动执行的特点满足了交易双方的履约需求，实际上赋予了债权人优先受偿权，具有担保性质。〔34〕(2) 关于智能合约的内容和形式，内容上应该主要体现为交易流程以及发生的法律后果。形式上应该以法律语言为主，从而对智能合约下的证券交易进行法律验证，从而体现交易主体的真实意思表示，明确交易双方的权利义务关系。(3) 关于智能合约的备案审查制度，目前智能合约的一大风险是合约代码可能会出现漏洞，遭到攻击或在出现争议时责任主体不明，而合约由一套代码组成并自动执行，有时很难查证智能合约在技术设计上和内容上的风险，只有事先备案，才能使纠纷在发生时得以快速解决。(4) 关于智能合约的中止和终止执行机制。智能合约不可以修改和撤回，不具有灵活性，但是中止或者终止执行合约的情形十分多见，比如发生不安抗辩权的条件下会涉及智能合约的中止执行，在混同、合同一方完全丧失执行合同能力时需要终止执行。因此有必要考虑使其中止或终止的程序化设计。〔35〕在智能合约编程时通过阈值的设置〔36〕来实现一种“失效安全”机制，即授权相关主体在满足特定条件时中止或者终止智能合约的执行，是一种可以考虑的做法。〔37〕

（三）结算最终性时点不明：六次验证

结算最终性原则是指在结算具有最终性的时点前，已经结算和已经发出结算指令的证券交易不可撤销，在此时点后，未经发出结算指令的证券交易也不得被撤销，证券的交易发生结算效力，该结算不因存在其他债权债务关系而受到影响，尤其是不受破产法上的撤销权影响。结算的最终性是证券结算风险管理的关键要素。涉及资金和证券何时在系统中发生所有权的转移、证券交易何时不可撤销，进而也涉及金融风险的转移。〔38〕在区块链技术下的证券结算系统中，证券交易依赖于区块链中的节点通过共识机制进行验证，只能随着验证数量的增加来保证结算的最终性，并且随着时间的推移，证券交易会 100％被确认并实时结算，但是仍然需要确定结算最终性的时间点。因为，缺少结算的最终性，会使已经达成的交易可以被撤销的时间不明确，一旦参与

〔33〕 See Trevor I. Kiviat, Beyond Bitcoin: Issues in Regulation Blockchain Transactions, 65 *Duke L. J.* 607 (2016).

〔34〕 参见倪蕴帷：《区块链技术下智能合约的民法分析、应用与启示》，载《重庆大学学报》(社会科学版) 2018 年第 6 期。

〔35〕 See IOSCO Research Report on Fintech, 2017, p. 52, available at http://www.iosco.org/library/pubdocs/pdf/IOSCOPD554.pdf, last visited on Dec. 26, 2018.

〔36〕 参见前引〔13〕，刘瑜恒、周沙骑文。

〔37〕 See Cheng Lim, T. J. Saw, CalumSargeant, Smart Contracts, Bridging the Gap Between Expectation and Reality, Oxford Business Law Blog, available at https://www.law.ox.ac.uk/business-law-blog/blog/2016/07/smart-contracts-bridging-gap-between-expectation-and-reality, last visited on Feb. 26, 2019.

〔38〕 See Principles for financial market infrastructures, IOSCO, 3. 1. 6, (2012).

结算的一方发生破产，会对已经发生的交易能否构成破产法上撤销权的对象产生争议。

本文认为，经过六次打包成区块验证的交易时间宜作为证券结算最终性的时间点。主要原因是：(1) 虽然区块链下的证券交易可以实现实时结算并不可逆，但是交易的不可逆特性依赖于节点的验证，并且经过的时间越久，交易就越不可逆。且从技术上看，一般认为，证券交易经过六次验证并打包成区块后基本不可能再更改。(2) 确定证券结算最终性的时间点一方面要考虑保持证券交易权利义务关系稳定性和证券市场流动性，另一方面，则要考虑证券交易验证的时间。目前运用区块链技术的主流的数字货币——比特币和以太币的打包时间分别为 10 分钟和 20 秒，并且随着技术的进步，时间可能会更短，六次验证的时间不会太长，并且能保证交易基本不可逆，基本不会受到破产法上撤销权等的影响。(3) 将经过六次打包成区块的时间点作为结算最终性的时间点平衡了证券交易发生后交易对手破产的风险，既能维护证券交易的确定性以维护证券市场的稳定与安全，又考虑到了证券交易中的破产方债权人的保护问题。

(四) 法律责任不清：立法明确

在区块链下，由于区块链弱中心且多中心的特点，在出现市场摩擦时会产生由谁界定责权、如何界定等新问题。因为没有主体能够控制该技术的运行，所以在发生损害后如何分配责任成为难题。而且这也会增加投资者权益保护和维权救济的难度。良好的责任分配机制不仅可以使得责任发生后相关主体的权利得到救济，而且有预防损害发生的功能。责任机制的缺失，则会给在证券领域应用区块链技术留下隐患。首先，没有承担责任的风险，技术开发、运营和维护主体就不会像在有责任压力下那样谨慎地研发和维护区块链，而只是在商业利益的驱动下开展工作。其次，在出现风险事件时，相关主体可能不会积极主动地予以处置，而任何主体提出的危机解决方案，在缺乏权威性的情况下都可能被否定或者耗时太长，不利于对风险事件的及时处理以降低风险、减轻损失。最后，在侵权问题发生后，由于区块链技术的系统中各方利益错综复杂，责任难以划清。在法律缺乏明确的责任分配机制时，在何种情形下由谁来承担何种责任没有明确的规定。过错责任、过错推定和无过错责任在这一问题上也无法准确界定。一旦危害发生，涉及责任的有无和大小时，将会是一个十分棘手的新问题。因此，区块链下的证券交易结算的各方法律责任急需厘清，这不仅是促进新技术良性发展的要求，也是防范证券交易结算风险、保护交易各方利益和维护证券市场稳定的必然要求。

区块链中的证券交易结算涉及的主体主要有：开源软件的编制及维护者、区块链系统验证节点、证券交易结算服务者和参与者。要解决法律责任问题应该从各方的法律关系入手。第一，软件的开发者亦是维护者提供证券交易的基础设施，与证券交易结算服务者和直接在区块链上进行交易的交易参与者应该构成服务合同关系，在区块链存在系统安全风险而导致被服务方遭受损失时，软件开发者应该承担瑕疵给付或者侵权责任，当然在赔偿上受到过失相抵、损益相抵和可预见性规则的限制。在归责原则上，应该适用过错推定原则，一旦软件开发方无法证明自己没有过错就要承担相应的民事责任。第二，当智能合约在运行过程中因错误或漏洞产生纠纷，应当由智能合约开发者和智能合约运行平台共同承担不真正连带责任，因为智能合约的安全性关系到整个证券交易的安全，证券交易方是智能合约的直接使用者，因智能合约的漏洞而导致的交易方损失应由智能合约开发者承担侵权责任，同时交易平台在此过程中有审查不严的责任，应该共同承担

连带责任，但是因为损失产生的根源在于智能合约的开发者，所以应该允许平台在承担责任后向开发者追偿。平台所承担的是一种中间责任而不是最终责任。〔39〕受损害的证券交易方可以要求智能合约开发者和智能合约运行平台承担责任，而最终只由智能合约开发者承担责任。系统维护者的赔偿只是一种“预付”，在行使追偿权后便可全身而退。〔40〕这类似于因生产者过错而导致消费者受损时的产品责任归则原则。第三，区块链系统的验证节点作为维持系统运行的主要参与者，某一节点的验证会受到其他节点的反复验证，因此实施欺诈验证的可能性并不大，但也不能忽视。本文认为，应惩罚那些故意实施欺诈验证的节点，取消其参与验证的资格，并由其对因其欺诈验证而导致的损失进行赔偿。第四，区块链应用于证券交易结算还会涉及行政责任乃至刑事责任，即损害产生是否涉嫌证券市场的欺诈、内幕交易和虚假陈述，如果答案是肯定的，那么则应追究行政或者刑事责任。

在法律责任的构建中，应明确各方参与者的法律关系，从法律关系出发，形成严密的追责机制，避免损害无从补救、责任无人承担情况的发生。这既是保护投资者和其他参与主体利益的需要，也是维护证券市场安全的要求。

Abstract: As a representative of newest technologies, the blockchain technology can realize the goals of owning securities directly, updating data synchronously, settling securities automatically and flexibly and improving security when applied to securities settlement, which can overcome the shortcomings of high costs, low efficiency and poor security in traditional securities settlement. Among the current three main application modes, the sharing among core institutions model has strong application value, since it can achieve the value of efficiency, cost and security and match the traditional securities settlement by overcoming the weaknesses existing in fragmented mode and completely non-intermediary mode. At the same time, it is necessary to implement embedded regulation, manage the smart contract from multi-angles, define the completion time of the sixth verifications as the settlement finality time and make Legal liability for securities settlement under blockchain technology clear.

Key Words: blockchain, settlement reform, application mode, smart contract, embedded regulation

（责任编辑：周　游　赵建蕊）

〔39〕 参见杨立新：《论不真正连带责任类型体系及规则》，载《当代法学》2012 年第 3 期。

〔40〕 参见税兵：《不真正连带之债的实定法塑造》，载《清华法学》2015 年第 5 期。