

# DTCC

Securing Today. Shaping Tomorrow.®

2016年1月

## 勇于突破 把握机会

释放分布式总账的潜力，  
完善交易后处理的格局

行业白皮书





# 目录

引言 .....	1
摘要 .....	2
当今金融市场的演变.....	4
现行金融市场基础设施的局限.....	5
区块链和分布式总账的主要特点 .....	6
如今分布式总账技术的现状 .....	8
金融服务业利用分布式总账的组成要素.....	10
发挥分布式总账的作用 .....	12
结论 .....	18





# 引言

DTCC是一家金融市场基础设施公司，由行业所拥有和治理，在帮助金融业缓释风险，提高运营和成本效率方面拥有40多年的丰富经验。我们认为，分布式总账技术承诺的实现有赖于将技术与这些核心原则统一起来，把握新的机会，简化或代替遗留系统。

比特币支付网络<sup>1</sup> 及其相关区块链(blockchain)、侧链(sidechain)和竞争链(altchain)生态系统的横空出世，一直被描绘成金融服务业的划时代突破性力量。分布式电子货币的概念至少早在20世纪90年代即已存在<sup>2</sup>，但比特币及其描述白皮书的广泛使用才是去中心化加密货币使用、采纳和普及的分水岭。业界对比特币支付机制已经有广泛的讨论和研究，而在本白皮书中，我们主要侧重于比特币技术平台(也就是通常所说的区块链或分布式总账)，作为金融市场基础设施所管理的交易后处理和其他功能的实现。

比特币平台的前提是一种去中央化、无需认证、自动复制性的交易总账，与长期以来依赖DTCC等中央机构的中央化、认证认证的、有监督的现代证券处理模式恰恰相反。认证模式加上对共同后台流程的集中处理所带来的规模经济效应，以及对6的严格控制和行政监督，保证了即使在极端性成交量和系统性市场震荡时期，证券交易处理同样安全、可靠。此外，它也建立了世界上成本效率最高的交易后处理基础设施。

DTCC一直致力于推动创新，完善交易后处理流程。为此我们不断探索将分布式总账技术应用到多种处理的可能，为行业进一步降低风险和成本。本白皮书希望能化繁为简，去伪存真，通过DTCC的慧眼探究利用分布式总账技术来完善现有商业模式和遗留系统的机会。DTCC维护市场的核心使命，代表着安全、稳健、完整、坚韧、可靠，DTCC通过40信任，始终是这些思想的核心。

1 比特币：一种点对点的电子现金系统 <https://bitcoin.org/bitcoin.pdf>

2 D. Chaum在1983年提出的ecash(电子现金)，A. Back提出的hashcash(哈希现金)，1996年推出的E-Gold(电子黄金)

# 摘要

如今全球金融市场依托复杂的内部系统和服务供应商网络，支撑着每天数以亿计的金融交易。内部和外部系统交错，看似杂乱无章，但经过多年的不懈努力，已经浑然一体，实现资产、信息和数据跨市场和跨地区的无缝高效流动。现行系统虽未基于预先规划架构和设计创建，但仍提供了必要的稳定性、可靠性和确定性，保证了全球市场的高效、透明和成本效益。

DTCC认为，分布式总账技术利用共享的通用信息结构，对金融行业基础设施的不连贯式设计进行升级、梳理和简化，有可能会解决现行交易后处理流程的部分局限性。凭借这一技术的多个关键功能，它有可能成为完善现行流程的理想方案，包括标准的证券交易验证和复制规则；持久不变的交易历史的延续和可审计性。

分布式总账技术虽然抓住了行业的想象力，但在达到普遍采纳或企业应用阶段前，还需要克服一些关键的挑战。此外，行业本身也需要确定与提升现有技术平台相比，使用该平台的成本效益是否更高，是否可以克服其固有的规模和性能挑战。另外还需要开展全行业的讨论，包括监管部门和决策者的参与，就开发要求达成共识，确定可以信任的第三方是否能提供最佳的方案。

行业对这种新平台的宣传和研究前所未有，但整体上仍然杂乱无章，或会导致历史的教训重演，依据不同标准建立若干新的不连贯式解决方案，统一协调将会极其困难——新系统将会面临的挑战将与今天一样，为此行业应当携手重构核心流程和惯例架构以确保标准化。DTCC相信我们完全有能力支持和协调分布式总账平台的评估和标准化工作，帮助解决行业挑战，确定它是否与现有技术相比是更好的方案。此外，DTCC作为一个由行业拥有和受监管的金融市场基础设施，拥有40多年缓释风险以及提高运营和成本效率的经验，以服务行业、监管部门和投资者为出发点，真正重视交易后处理的利益，具有履行这一职能的独特优势。

在评估利用分布式总账来完善现有基础设施的机会时，DTCC已经确定多个需要进一步研究的领域和流程。根据研究和分析结果，DTCC建议探索在以下领域应用分布式总账技术：

- 主数据管理
- 资产/证券发行和服务
- 确认资产交易
- 目前还不具备完整解决方案的复杂资产类型交易/合约的验证、登记和比对
- 净额结算与清算
- 抵押品管理
- 结算

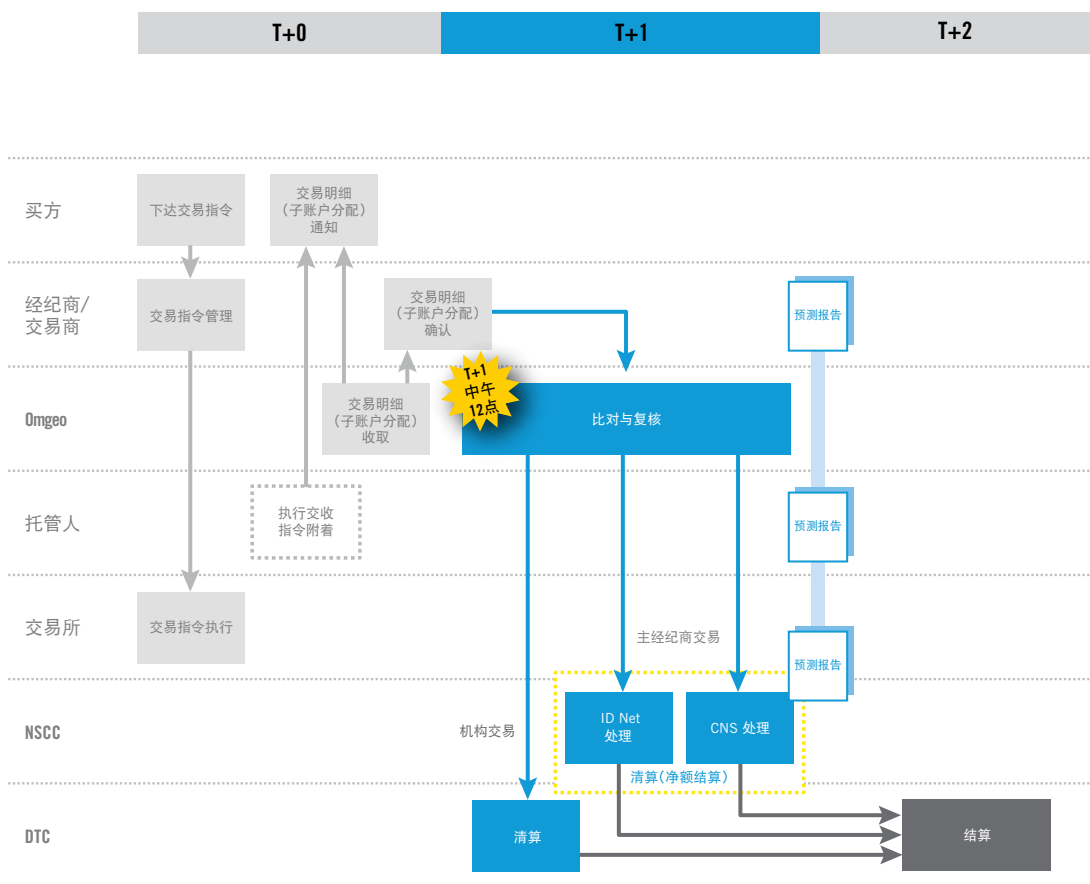


尽管对于分布式总账技术在实时结算方面的应用已经有了大量讨论，但根据法律规定和市场架构，目前美国股市采用T+3交割制度。为支持实时结算而对现行惯例和法律进行提升和改变，与是否应用区块链技术没有任何依存关系。

DTCC坚信，在重新想象和升级基础设施，解决长期困扰的操作问题方面，金融服务业面临千载难逢的良机。DTCC有经验和能力按照符合其使命并进一步降低所有市场参与者风险和成本的方式，支持金融业分布式总账生态系统与现有金融市场基础设施的整合。

## 当今金融市场的演变

最基本的交易十分简单，投资者交换有价值的资产，收到作为对等的付款。点对点，无中介，理论上实时交换。这就是早期证券交易所的交易方式，交易协议和结算一般会由双方实时完成。随着交易所的不断成熟和日渐复杂化，加上越来越多的人积累资产并授权其信任的第三方代为持有和管理资产，不同的服务供应商被委托来负责处理交易的每个流程。但经常由于被委托的服务供应商滥用投资者资产，金融危机周而复始地发生，投资者损失惨重，提升治理能力和使用公用事业类基础设施应运而生，以监督处理和减轻这些损失及其他风险。因此而带来的是今天的交易层级十分复杂，如下图所示，它是目前美国计划将结算周期缩短至交易执行后两个交易日，即T+2的流程图。



上图对各公司的具体处理流程进行了简化。在现实世界中，买方和券商/交易机构的系统错综复杂，综合了过去40年通过自动化处理的优化、监管要求和市场演变等途径开发的各种系统。今天交易委托管理、交易后处理、资产账户服务和数据管理等不同操作，均由不同的内部系统和/或服务供应商提供。尽管存在多个层级的复杂交互、对账与工作流程，现代全球市场仍实现了较高的效率和透明度，成本相对较低。



# 现行金融市场基础设施的局限

如今金融市场基础设施在稳定性、可靠性和可确认性上都表现出色——这些都是保证市场高效运行的关键，尤其是在极端波动期间。雷曼兄弟(Lehman Brothers)和明富环球(MF Global)破产、2012年“电子交易故障”和2010年闪崩事件等近年发生的案例，就很好地凸显了发生系统性动荡时，中央对手方和市场基础设施在保护全球金融系统完整性上起到的关键作用。但现行系统也存在一些局限性，而这些局限性有可能通过分布式记账的技术来解决：

- **多个版本的数据：**金融市场系统的层级被相互孤立，包含多个版本的数据。各个系统的透明性极低，每家银行都有规模巨大、成本高昂，但其存在仅仅是为了核对不同版本数据的应用程序代码库。
- **应对技术威胁的能力极为脆弱：**目前所采用的旧的系统在架构上并未考虑防范当今的技术威胁，包括潜在的网络攻击威胁。因此系统漏洞的存在可能会导致数据泄露。
- **不必要的复杂性：**现行系统经过数十年的演变，变得极为复杂。交易活动以及清算、结算和抵押品/资本/资产管理系统，建立于不同的时期，满足不同的需求。许多标准的使用范围极为狭窄，系统集成性不佳，甚至仍然存在许多人工处理环节。
- **不具备全年不间断处理能力：**现行系统的架构大部分都是在行业全球化之前设计的，并不支持因此所需的市场全天24小时，每周7天，全年365天无间断运行。

# 区块链和分布式总账的主要特点

在评估有哪些范畴可以利用分布式总账来完善现行证券交易处理系统时，首先需要了解比特币支付网络以及构成其底层技术平台的具体要素。

比特币支付网络是一种点对点、分布式、去中央化的平台，用于验证和追溯交易，无需任何中央机构。建立这种创新的平台需要具备如下八个关键功能：

- **资产内置：**资产被称为比特币(BTC)，完全在比特币网络中生成和管理。因此，比特币每次移动的历史和数量都可在比特币网络的分布式总账中，利用记录的历史从数学上验证。
- **当事人身份抽象：**以隐匿性保证安全性，这一特点内置在平台中，意味着永远无法识别当事人的个人身份。相反，查看交易输出必须提供安全密钥(公开密钥和私密密钥对)。仅私密密钥的持有者可以发送比特币或查看收到的比特币，仅私密密钥的持有者知道他们所拥有的比特币总量。
- **交易链：**每条交易记录(总账分录)都链接到之前的交易，并以标准化的方式支持每个参与的节点。每个总账分录都可按其完整的历史追溯，可以重新构建。
- **交易脚本：**交易脚本是交易所适用的标准化规则和条件，每个节点都适用相同的规则。在简单的比特币模型中，比特币根据规则从一个当事人移动到另一个当事人。更新版本的区块链扩大了这些规则的范围和能力，构成所谓“智能合约”的基础。
- **交易分发：**利用一种标准的网络协议，每个参与的节点都可收到每项交易，执行同样的验证规则。
- **区块链：**这是规定各个节点如何存储交易数据(总账数据)的唯一标准，每个节点都遵守该标准，可以拥有该数据的完整副本。因此有时人们称之为“分布式总账”。记录(即交易区块)添加到区块链上，包含与之前所添加区块的链接。这是最终的、不可变的交易记录。
- **去中央化的共识：**它是由各个节点如何交换区块链信息的标准和规则、所有节点接受数据的完整性的数学逻辑(有时被称为“工作证明”)以及支持共识模型的付款激励组成。此模式及整个平台的关键在于确保所有交易都得到验证，并且所有有效交易都添加一次并且仅添加一次的方法，不会遗漏任何有效的交易(有时被称为审查制度)，在比特币网络中，一个比特币无法花两次。
- **认证与无认证，授权与非授权：**“无认证”模式是指基于互联网的公开、开放式访问性而搭建的比特币网络。任何人都可下载开源的软件并加入。比特币网络在搭建时不认证任何节点，其模式是只要多数(51%以上)节点作为诚实的参与者参与上述共识活动即属有效。认证或者授权是对这一模式的重大修改，被提前授权的服务器只有在获得批准后才能上线进入该网络。

简而言之，区块链是一种网络和数据库；它拥有规则和内置的安全设置；它维护内部完整性及自身的历史记录。这些因素创造了比特币区块链的价值，上述每一个概念都有单独使用，或以不同的组合使用，从而完善现有金融交易处理的潜力。

比特币网络提供近乎实时的结算，属于一种独特的创新。我们将在后文中进一步讨论，实时结算可以使用现有技术实现，对于部分资产类别已经实现。目前美国权益类市场整体上采用T+3制度(交易日后第三个工作日进行结算)，行业正在计划改为实行T+2，这些并非是因技术局限所致，而归咎于法律和市场结构的原因。为支持实时结算而对现行惯例和法律进行升级，并不依赖于是否使用区块链技术。

# 当今分布式总账技术的现状

直到最近，一些金融市场的前沿创新者和策略规划师才转变思维，从分布式总账对加密货币交易的具体应用，转向使用该技术来支持其他金融和证券行业处理工作。虽然目前正在进行许多试验，使用情形也有多种，但尚没有一个分布式总账应用程序大规模投入现实应用。这部分归咎于与规模、延时、性能和安全性等有关的根本技术挑战。此外，与操作、登录和监测工具的集成等非功能性要求，对每个企业生产环境都至关重要，但这些集成问题还没有解决。现实情况是在所有进行的开发试验中，在这个领域有丰富运营经验的、知名的技术厂商极少(如果有的话)。因而这些创业厂商的产品质量、企业支持能力和实际长期生存能力都需要完善，以促进该技术的发展。

新开发、新合作、新联合体近乎每天都在宣布，有关该技术进步的新闻也持续曝光，但在所有这些宣传之外，该技术的应用实际上仍处于极早的初期阶段。到目前为止，市场上存在各种不同的实现方式、不同的规则、不同的数据和安全模式。此外也没有广泛被接受的标准，虽然在此领域有很多参与者正在努力，但问题的解决绝非一夕之功。对下一个大突破的讨论说明大规模的采纳迫在眉睫，但事实却并非如此。实际上，分布式总账最多被认为是证券交易处理领域的一个新兴技术。

## 分布式总账技术的局限

在评估分布式总账对交易后处理的应用能力时，我们需要了解今天所用的分布式总账只是一个简单的交易总账，基本上就是复制交易到所有合作服务器上。该技术并不具备与现有系统和配套基础设施内置集成的能力，它不能方便地与用户身份管理系统集成，也不拥有有关法人机构或证券的任何主数据。它不包含配套的工作流程、异常处理或广泛接受的预处理逻辑，也不支持复杂的比对、子账户分配和其他处理，而所有这些流程都是一个完整交易的必要执行步骤。

分布式总账平台的一个宝贵功能是所有交易都被视为不可改变，永远不可修改、取消或撤销。但在现实世界里，客户更正/取消/调整因疏忽被错误收费或划入错误账户的情况，是一个十分普遍的现象，金融机构在此方面的管理也得得心应手。此外，复杂的金融交易常常包括根据合同规定的反转交易的可能。目前的分布式总账平台并不支持取消或反转交易，目前尚不明确该平台将如何进化来支持这些需要。

此外，该技术在以下其他领域也存在一些缺陷：

- 它在现有数据的检索、查询、报告或分析工具方面没有任何提升的作用。
- 它不允许按照与现代数据库类似的方式搜索数据。
- 它不能以与大数据技术相同的方式高速访问数据，以进行数据分析。
- 它不能与现代数据管理工具集成。
- 它不能解决大部分操作系统的非功能性要求。

如果要把分布式总账全部潜力发挥出来，所有这些存在于现行交易后处理流程中，由专家和从业人员多年努力建立的功能，需要集成到这一新的平台中。

## 去中央化与中央化处理

考虑是否广泛应用分布式总账时，另一个重要的考虑因素是权衡去中央化处理与更为传统的中央化处理计算模式的优缺点。

从定义上看，去中央化处理是社群成员(无论是认证的还是非认证的)之间的一种共享计算功能，要求同步和协调。分布式总账的部分应用方式，例如比特币，使用共识机制来管理协调问题，而其他应用方式则使用带头节点机制等变化。尽管如此，所有这些设计都包含添加交易处理延迟的环节。去中央化设计要求极大的计算和存储资源，因为所有节点都要执行计算并存储总账数据，根据网络节点数量以及每项交易的规模不同，这可能会导致网络带宽要求大幅增加。

而与此相反，使用中央化处理，只需一个真相判断，即可一次查看信息，通常只需一台机器。这种模式的延迟几乎为零。当然分布式总账平台的部分原理仍然是可以借鉴的，也可以在中央化的系统中实施，例如更好的安全性、标准化的验证规则和可验证的交易历史的特点。但这种模式也要求完全认证中央化系统和管理该系统的组织的完整性来实现。

全球有关数据隐私保护的监管要求有极大的地区差异，是去中央化系统面临的另一个挑战，因为这些系统会向每个节点分发所有交易。在部分监管地区，个人数据隐私保护法律对在受监管地区之外存储特定的数据有严格限制。部分厂商最近提出了替代的“分区”总账概念来解决这些挑战，但由于目前有关分布式总账的所有工作都没有监管机构的监督或认可，因此对于存储在其他地区数据的限制目前尚不清楚。

对于金融业而言，理想的未来状态到底是目前使用中央存托机构和托管人等需承担责任的中央机构的惯例，还是使用数学和加密技术来保证完整性的分布式系统更佳，这一问题尚没有答案。未来状态可能会要求同时具备这两种形式的处理。DTCC认为，该技术可以用于支持以上任何一种方案，而最符合逻辑、风险最低的方式将是由现有受监管、受到普遍信任的中央机构推出标准、治理架构和技术，以支持分布式总账的实现。引入现有的受监管的机构，自然会涉及监管部门参与并支持可能需要的潜在政策调整，以促进这一技术的成功。此外，我们认为该技术和总账应当由行业所拥有，从而能与整个行业的需求保持高度一致，机会也主要集中在尽可能有利于整个行业的方面。

# 金融服务业利用分布式总账的组成要素

尽管存在上一章所提到的局限，DTCC认为一个安全的分布式总账，如具备完整、可追溯的资产交易历史，在受认证的当事人之间共享并仅供受认证的当事人访问，则可显著完善当今基础设施的特定领域。它通过以下方式支持解决方案，解决当前面临的商业挑战：

- 一个共同、共享的真相版本——每个受认证的会员都拥有相同的资产全部交易历史。
- 所有数据都按照符合现代标准的常见方式加密，仅可以由数据密钥的所有者解密和查看。
- 共享的总账由参与具体资产交易的每个受认证的当事人使用，**建立了一个网络和数据标准，以简化、统一的方式与工具、工作流程和资产管理系统集成。**
- 交易分发模式采用始终在线的双主动模式处理，与现行硬件复制模式相比对于本地数据库的崩溃具有更好的耐受能力。

在金融服务业利用分布式总账涉及多个关键的要素，包括全行业接受并采纳经证实定义的，将在分布式交易总账中编码的金融工具、法人机构和金融合约标准。**一个至关重要的核心要求是分布式总账“认证边界”的治理和监管框架。**认证边界是指总账与非总账内部任何事物集成的位置，例如认证主体作为总账会员开户，或赋予任何主体向总账中签发资产的权力，以及验证对具体资产的权利是否由该主体所有，并且相关资产在总账外是否得到恰当保护。分布式总账可以提供一项资产不可变的数字记录以及该有价值资产的交易过户，与总账网络中的其他当事人共享。但如果资产本身属于实物形式或未直接并完整存储在总账中，资产托管人仍将享有中央化的认证，以确保资产的真实存在、得到保护并且未被输入到多个、未连接的共享总账中。

**管理标准、规则和认证边界的关键职能，必须以无可争议的完整性和责任性进行，独立于任何商业冲突。这正是DTCC等行业基础设施组织已为金融市场提供了四十多年的职能。**

## DTCC在如何使用分布式总账技术中发挥的作用

DTCC认为自身是潜在向新的分布式平台模式转变的助力者，促进更好的安全性、适当的透明性和更高的可靠性，可以减轻风险，简化整个金融业的处理。作为一个由行业所拥有和管理的基础设施机构，DTCC可以促进金融业分布式总账生态系统与现有金融市场基础设施的集成。DTCC认为以考虑尽可能充分、风险和测试尽可能得到恰当管理的方式，推出新的平台，这一职能与我们推动创新的使命和职责一致。

DTCC还认为，使用共享的分布式总账信息结构记账有能力提升、梳理和简化现行金融业基础设施的**不连贯式的设计**。为了实现这一目标，需要整个行业携手来重新设计经过数十年时间搭建的核心行业流程和惯例架构，这些流程和惯例各不相同，要求与之前和未来的系统进行核对。使用分布式总账技术而进行的协作化的行业现代化整合可以减少金融交易所需的流程环节，提高所保留处理系统的安全性和坚韧性，从而降低成本和交易失败的风险。



## 以史为鉴：协调与标准化是关键

去年，许多行业参与者已经开始进行单独的试验，建立一个个孤立的专属合作关系，一窝蜂地将不同的总账机会产品化，情况十分混乱。这是自由市场关注短期收益机会的固有本性，目前金融市场基础设施的杂乱无章正是这种毫无协调的实施、市场机会和监管应对的苦果，如果继续下去，历史将会重演。

行业多年来被迫投入大量的精力和资源，试图解决因缺乏协调、合作和标准化导致的问题。随着金融机构考虑将运营迁移到分布式总账基础设施的机会出现，在相当长一段时期内将需要连接现有的基础设施并且与现有基础设施共存。互联的完整性和稳健性是确立对新基础设施认可的关键。建立无限数量的不同总账的独立存储，将会增加成本和复杂性，可能实际上会增加系统的风险。该技术的全球覆盖性和相关限制也导致与全球不同监管地区有关的挑战，但也可能会促使全球决策者相互合作，建立支持新机会繁荣发展的法律框架。

## 知识产权






与这一新技术有关的知识产权也需要谨慎考虑——开源和统一标准是原始区块链实现前提的一部分，必须与专用厂商方案的商业格局所固有的利益平衡。一个能够服务整体市场的可持续分布式总账平台，应当要求中央式的行业协调和治理，不论是通过行业协会、公开论坛还是以服务行业为使命的行业公用事业机构为主导力量。

## 企业集成

DTCC坚信，重新构建金融行业的基础设施是一个划时代的机会，这只能通过经过精心考虑、协作和设计的方法实现。可能的第一步将是定义相关的基本要素，以将交易总账集成到企业中，例如与现有金融机构信息系统、用户身份识别系统和资产信息系统集成。

# 发挥分布式总账的作用

以下是DTCC对分布式总账技术如何能够完善现有基础设施的一些观点。根据我们的总体评估框架，我们针对各个商业领域机会，评估了认证的分布式总账所具有的下列优点。

<b>标准：</b>	 分布式总账是否有助于强化行业数据格式和合约规则的标准化？
<b>效率：</b>	 分布式总账是否能消除人工交互、数据交换、数据格式转换以及与其他系统的核对要求？
<b>更快操作：</b>	 分布式总账技术能否提供一个平台，减少交易完成的时间和风险？
<b>透明性：</b>	 分布式总账提供的透明性是否有利于对该技术的商业应用？
<b>安全性：</b>	 分布式总账所固有的认证和加密能否提高这一业务流程及其数据的整体安全性？

DTCC认为与现有的技术相比，这五个特点将是认证的分布式总账可以实现的最关键、最重要提升之处。当然分布式总账平台的其他方面目前也在测试或研究中，例如公开透明性、激励挖矿和用户匿名性，但在受监管的市场里，这五个优点最值得评估。

如上文所指出，该技术目前面临诸多局限，妨碍了许多金融交易以灵活方式使用该平台。这包括单个交易的规模和可以同时写入的交易数量等方面的限制，以及写入总账与最终确认之间的延迟等。但目前所开展的研究和试验可能会打破这些局限，从而有利于广泛使用。本白皮书着眼未来，认为这些局限将被打破，因此在剩余的讨论中将忽略这些局限。

一个重要的问题是能否实现与现有技术同等的效果——减少风险和降低成本。这一问题只能在试验和试运行验证了分布式总账技术的能力和局限后，才能全面回答。本白皮书和本节的前提是，分布式总账方案中实现了上述五个特点，可以在涉及超过两个当事人时，提供更有用的记录保存、交易处理和交易价值转移方案。

本节分析了支持交易处理的信息来源的不同基本要素类别，考虑了是否要求单一的认证的中央信息来源，还是可以利用去中心化总账方法的优势。与现有数据管理平台相比，总账技术确实提供不同的能力，但它们并不总是放之四海而皆准的真理。任何有关重新构想金融业的讨论，必须考虑现有技术哪些方面仍能充分满足所要解决的问题需要。

## 记录保存： 身份管理

身份和访问权限管理系统是每个金融业基础设施的关键组件之一。在每个金融企业中，将用户身份与其资产持仓账户(或比特币钱包)关联起来，都需要执行开户流程。提供身份信息要求安全的认证来源，部分当事人会验证生物信息或其他物理信息和资料。此外还有重要的监管考量因素，尤其是在非公开的个人身份信息因素保护方面。在拥有单一的真相来源，对于所有前台、中台和后台应用程序实行严格集成的金融企业来说，身份和访问权限管理系统往往是一个与其他系统高度集成的系统。身份和访问权限管理系统及其非公开的个人信息和金融持仓密钥，也成为最受关注的黑客攻击对象。

当前的现实是，被认为无懈可击、极其安全的系统正在较为轻松地被攻破。由于分布式总账技术属于新生事物，在其成熟并证明其承受攻击的能力前，与身份有关的数据不适宜存储在去中央化的分布式总账中。

## 主数据管理

法人信息、资产信息、交易日、节假日信息，以及其他常常使用的非交易性商业信息等等的主数据，是所有证券交易处理的基本要素。该信息一般包含企业自己维护的主数据，以及属于整个行业共有的主数据。目前大部分主数据系统都具有专属性质，针对当地企业的要求，极少(如果有的话)有共享的标准，实际的数据更为稀少。这是整个金融行业许多对账工作的源头，当然也是许多企业内部独立系统之间对账工作的源头。

DTCC的观点是，基本的行业主数据是使用去中央化共识机制、规则标准化和可审计的变更历史来进行完善的理想对象。该信息由整个行业自定义使用，缺乏一致性，质量问题长期困扰着市场参与者。此外，其构建方式可采用多个被认证的企业作为数据提交者，可以有多个数据验证者，大部分用户将是数据消费方。但应当指出的是，部分区域性的法律具体要求主数据信息是以不可编程的法律用语编写的，将对未来支持规则自动化的标准化工作带来挑战。

与主数据管理有关的另外一个方面，包括了要求支持以安全方式访问的分布式总账基础架构，也就是公开密钥基础架构。将公开密钥与法人身份关联起来的认证常用机制，可能是分布式总账基础架构至关重要、极有助力的要件之一。公开密钥的分发似乎是为分布式总账技术量身定制，已经成为其他测试的对象<sup>3</sup>。

## 资产/证券发行和服务

拥有统一、广为人知的资产完整所有权起源的信息来源，对资产发行人以及这些资产的所有者的好处十分明显。使用分布式总账来管理证券发行并跟踪当前的所有权，可以极大地简化资产服务工作，而使用旧的中央化技术难以实现。一个重大的挑战将是插入到分布式总账中的资产，与已经以原有形式记录在总账之外的资产之间的整合，例如存于托管银行或DTCC等存托机构的资产。按照符合投资者保护相关监管要求的方式解决这一挑战，是之前所定义受认证边界的一个例子。在这个例子中，受认证的资产托管人是集中处理行业职能的一部分，就像DTCC已经提供了40多年的职能，并且可以利用这一职能搭建登记中心与分布式总账之间的桥梁，从而支持从新的平台安全地接入在登记中心中的委托资产。

<sup>3</sup> Certcoin – 去中央化的公开密钥基础架构 <https://eprint.iacr.org/2014/803.pdf>

## 证券交易流程与智能合约：

以下的部分分析了属于证券交易生命周期一部分的诸多交易流程，并探讨是否可以利用去中心化总账方法的技术。

### 交易/合约验证、登记与比对

从定义上看，金融资产销售或交易是多个当事人基于合约基础上的协议。因此，如果可以用平台的规则充分体现协议，这些行为则可以通过去中央化的平台进行管理。足够丰富的合约条款语言，几乎可以覆盖任何资产的交换。分布式总账的潜在好处应当根据处理的不同方面，分资产类别进行考虑。

这一类别的范围包括(例如)多种基于合约的资产交易、基本的现货股票和固定收益、回购协议、跨所有资产类别的掉期交易、转账过户、银团贷款和可变年金等。

已确认的资产交易可使用分布式总账技术登记，而最佳的应用机会出现在尚无完备解决方案，涉及多个当事人的更复杂资产类型上。这些复杂的合约一般涉及多个人工处理环节和规则，这些都可以按照标准和格式化的编码来提升效率。如今的处理流程要求将数据转换后发送到另外一个系统，然后再进行验证，与符合合约规则的基准交易进行比对，由此带来的异常处理往往更为复杂。智能合约技术可以“事先”为交易对手方提供相同的验证规则，保障只有高质量、经过验证的数据才会进入到分布式总账，从而简化处理，提高纠正异常情况的效率。当然，确认内容、验证和协议规则的标准协商，要求很多的全行业协作。

分布式总账技术在交易验证、登记和比对方面的应用面临极大的障碍。例如，分布式总账仅包含总账以及确定写入总账的交易是最终、经批准/同意的验证——一次写入并且只写一次。并不包含主数据，没有途径跨数据库、无固有的工作流程和合约磋商，无针对常见真实世界中错配问题和异常处理的“比对”功能。比特币这种单一价值货币在当事人甲和乙之间流转的参考例子，并不能有效在涉及多达一千个可选字段，拥有复杂规则和交叉依存关系的多方资产过户的环境下充分发挥作用。分布式总账技术的价值在于，合约得到统一验证，然后写入分布式总账，“不可变”、含义不可更改、永远登记为最终合约。交易的修订、取消和更正则可能通过“逆向”交易解决。许多复杂的交易比对和异常处理工作对金融交易来说是十分常见的，但在这方面并不能使用分布式总账技术来天然替代。点对点方案或集中比对方案都可能继续占据总账前处理的重要位置。

另外的挑战来自各个地区的证券交易法规的不同，这些法规并没有全球统一的标准。当前的分布式总账技术将所有数据复制到所有总账中，无法根据地区法规要求来区分交易。可能需要使用分区机制将特定的交易限制在特定的位置，从而满足不同地区的监管要求。

最后，从实际角度看，必须承认目前自动化程度高、交易量大的资产类别可能已经达到规模效应，实现了风险的最低化。因此，实施全新的分布式总账技术并没有成本节省上的推动力。搬移到分布式总账而产生的运营中断和因此而带来的费用，可能不会为市场带来显著的效益，并且实际上可能增加成本和风险。

## 价值转移：

### 净额结算、清算

净额结算是参与资产交易的所有当事人之间的最优结算需求。清算对每笔交易使用中央对手方来简化多方净额结算，减少结算失败的风险。中央交易对手方(CCP)作为交易对手方参与每项交易——CCP是每个买方的卖方和每个卖方的买方。CCP将某一结算日期的所有交易进行轧差，计算出一个应付客户或应收客户的单一数量，可以判断客户无法履行其结算义务时的风险敞口。

净额结算和清算可以在适当的规则前提下，使用分布式总账的技术来实现结算的最优化。这些规则可以是中央交易对手方清算或替代净额结算方案。换句话说，从技术概念的角度看，净额结算和清算的功能可以用分布式总账技术实现。

使用分布式总账平台进行交易净额结算、清算和结算，将在下文讨论，跨过来自分布式验证和信息共享目的的门槛，进入许多提议者认为是分布式总账真正价值所在的领域——近乎实时的资产价值转移，独立于共同信任的第三方。越过该门槛，进一步深入分析目前基于中央对手方的流程的优点，以及分布式总账可以如何用于完善。

### 中央交易对手方

CCP已经成为现代金融市场风险管理的标杆。它们消除了交易当事人不执行交易合约的风险。它执行多边净额结算，极大地降低了需要执行的结算数量，减少了单一交易对手方的风险状况，从而降低了结算失败的风险。此外，它允许通过连接本身缺乏流动性而完成交易结算的买方和买方，为券商和其他代理人提供支持。因此，CCP对于建立稳定、坚韧、高效的市场和降低增提风险具有至关重要的作用。CCP的其他作用体现在资产负债表净额结算、担保未来结算交易的完成，例如回购交易，这些都促进了当今市场的顺畅运行，帮助保护市场度过破产和信贷危机，例如2008年的金融危机。

全球CCP的例子非常多，在本白皮书中，我们以DTCC在美国的股票和固定收益中央交易对手方作为当今金融基础设施的标准进行讨论。

DTCC系统的主要特点包括：

- **实时交易处理。**DTCC几乎在交易执行后几秒钟内就收到来自各个市场的每项交易明细。这包括了超过50家股票交易所和市场的交易。交易在申报后几秒钟内完成验证、比对并向客户返回交易确认结果。当日结算交易的申报(在当今T+3环境中的“即日”交易)直接进入实时结算系统。
- **处理规模。**DTCC平均每天处理超过1亿笔交易。DTCC在测试后确认其系统具备单日处理超过8亿笔交易的能力，是其历史峰值水平的两倍。



- **处理的成本效率。**在美国，DTCC的股票清算成本低至平均每笔交易几分之一美分，科技上的不断进步促使这一成本进一步降低。
- **互联互通。**美国资本市场包含50多家交易所和数千家金融企业，建立了非常成熟的互联互通系统，每天无缝运行。
- **净额结算效率：**超过97%的每日股票交易采用净额结算机制，剩余3%采用全额结算机制。总账模式对所申报的交易进行逐一结算，其成本和风险考虑因素需要结合现有中央净额结算模式的高效，以及并非每个交易当事人都可结算的事实。
- **更替：**作为中央对手方，DTCC减少了买方和卖方的风险，保证即使一方违约仍可完成交易。此外，DTCC还通过(包括但不限于)建立严格的会员标准、要求财务披露并对其客户执行金融监督，保证了交易伙伴的稳健性和偿付能力。
- **资产负债表内冲抵：**中央交易对手方清算为远期结算交易(例如贷款)提供了风险缓释效益以及财务会计效益，例如回购交易的资产负债表内冲抵，这些只有通过于与交易中央交易对手方进行清算时才能实现。

对于大部分现代金融市场来讲，这些因素意味着分布式总账技术必须从高起点出发。对于分布式总账技术的应用，发展中地区的金融市场可能有更多使用不同清算模式的全新机会，交易量的要求较低，风险容忍度也各不相同，这些都要求在技术应用上采用不同的方式。但短期内在发达市场难以看到使用这一技术的机会。如无明显的风险和成本降低优势，进行耗时、昂贵的更换甚至更为困难。

DTCC熟悉并且已经接触了多家建立发行/交易/结算/资产服务类的分布式总账的创业企业。DTCC作为行业拥有的市场基础设施，其定位是为所有符合条件的客户提供公平、开放的渠道，促进与任何有能力满足DTCC财务、风险和监管要求的客户对接。但如上文所述，DTCC对于将资产从中央化、有风险管理、受监管、治理良好的存托机构转移到使用专用结算和资产管理机制建立的众多零散厂商方案是否有积极意义深表怀疑。

## 结算

不同的交易采用多种不同的结算机制，从Fedwire支付和美国政府证券交易的实时券款对付结算机制，到复杂掉期和贷款交易长达数周甚至数月的结算等等。此外，许多交易涉及多个要求结算的“生命周期”事件，例如贷款，包括起始结算和最终结算等。

比特币加密货币作为价值转移机制十分成功，在不可变的总账上执行具有最终确认，证明在简单的情形下，券款对付结算机制可以编程，通过去中央化的共识网络近乎实时管理。

DTCC的股票和固定收益结算流程是全天候实时执行的，因此分布式总账本身并不能提高这部分效率。但重要的是，尽管DTCC的系统实时运行，市场本身目前的架构采用T+3周期运行(在交易执行后三个交易日结算)，主要是为了满足散户投资者的需求。因此，DTCC实时接收新的交易并在三天后处理交易的结算，延迟是因市场惯例、金融行业法律和监管要求所致。如上文所指出，在结算日申报的交易在三天前标记为“即日”，立即可以从申报进入实时结算流程，完成当日结算。



有些问题已经在2015年我们所发布T+2行业白皮书所提及，并做为改进的重点。该白皮书还强调了迁移到T+2所需的成本、复杂性和时间。分布式总账可能会进一步促进缩短结算周期至T+0，建立满足金融市场中不同参与者需求的机制和定价。例如，可以券款对付实时结算的点对点交易，其定价可以不同于需要中央对手方执行净额结算，以对冲经纪商头寸，承担对手方结算风险的经纪交易。这要求将大幅修改现行交易流程(例如合笔交易的子账户分配)、交易融资和多种其他内置的市场惯例。此外，交易处理能力、遵守金融行业法律法规以及从当前状态迁移到未来状态所涉及的复杂性和成本等问题也必须考虑。

分布式总账技术的标准结算模式可以反映安全、一致的当前资产所有权的真实情况，追溯资产的起源至托管人、代理人和受益人。这种单一的所有权真实情况的存在，可以简化资产服务工作，例如公司行为的处理、派发股利以及股东投票的管理等。尽管现有的技术可以提供所有这些功能，但仍要求复杂的交互和核对，这些工作可以通过分布式总账中的单一分布式真实版本进行简化。这种分布式总账的成功实现，要求所有资产都位于某个总账上，或者完全与所有链外资产汇总，包括这些资产所有的在托管行进行托管的历史，以及已经在其它链/总账上记录的资产。

目前尚未广泛建立结算工作流程自动化的资产类型，例如银团贷款，以及其他目前可能需要数周才能结算的交易，可以使用分布式总账技术解决。这些交易的合约和结算往往涉及多方当事人，所有当事人都希望以单一、一致的方式了解交易及其结算，这恰恰是总账技术的固有优势。

随着技术的成熟和扩展，结算可能是分布式总账的长期理想应用目标。需要考虑的问题包括修改法律、改变市场惯例和架构，顾及资产服务的复杂特点，与监管部门合作处理保护投资者利益等问题。DTCC认为，这是利用区块链技术的机会很重要的一个领域，此外也相信作为美国中央存托机构的托管人，我们拥有独特的优势，可帮助实现这一技术，促进其被更多市场参与者所采纳。DTCC会推动与行业以及监管部门的合作，确定战略路线图、治理流程和推进步骤，以全面超越现已存在的安全性和稳健性为标准。

将结算系统转移到分布式总账模式，要求行业进行大力投资，升级改造旧的系统，并投入资源，在一定时期内实现两个系统并存。但核对与简化对整体行业的好处，以及T+2计划和普遍存在的交易后处理的全新视角，都应该从行业效率和风险缓释的角度进行历史纵向评估。

## 抵押品管理

DTCC支持通过分布式总账进行结算和资产服务处理，包括在该平台上处理抵押品管理工作。资产起源、跟踪交易移动和真实所有权状况与临时/借贷(通过恰当的设计)的能力，是分布式总账技术得以广泛应用的根本所在。DTCC认为区块链技术的这一功能完全适合处理抵押品管理工作。

# 结论

现行金融行业基础设施具有极佳的坚韧性，克服了几十年来的许多挑战，它安全、稳定、可扩展性强、成本效益高，与整个行业联系紧密。它通过不断的创新以适应新的挑战，不论是交易量的攀升，自动化水平的提高，全球化，还是更多监管要求。它建立在金融市场基础设施的基础之上，特别是美国金融稳定监督理事会(FSOC)所指定的系统性重要金融市场基础设施机构(SIFMU)，必须满足最高标准的完整性、安全性、表现、可扩展性和坚韧性要求。它们经过几十年的考验，始终无缝高效运行，保证了全世界金融市场的顺畅运行。每天无缝发生的交易处理错综复杂，如有任何故障可能立即引发世界金融市场停滞，扰乱全球经济。对于这些基础设施的重大改进必须慎之又慎。

DTCC的结论是，一个成熟的、多方支持的、集成的分布式总账技术有潜力帮助改善现有金融市场基础设施的一些局限。但是，这也不是放之四海而皆准的万能药，因为通过行业工作流程的标准化，扩大云技术的使用，也可能有机会降低现行基础设施的成本和风险。

分布式总账技术的现状也面临自身的挑战：它还不够成熟，未经验证，当前形式存在固有的规模局限，缺乏与相关基础设施的链接并清晰地将其集成到现有的金融市场环境中。与所有新技术一样，随着时间推移以及行业吸取市场测试的经验教训，情况将会改善。

DTCC独特的股东结构和治理架构可以通过重点关注最基本的要素和商业使用情况，促进行业对这一技术的利用。针对尚未完全自动化的资产类别进行小范围技术验证和试点，可以检验该技术对解决全行业挑战的可行性。这些“空白”机会应当优先考虑，因为它们将为了了解这种备选模式的优点和教训提供最佳条件，无需对现有的基础设施增加不必要的成本。此外，它们还将减少系统集成和同时维护两个系统的挑战，无需努力解决已经被有效解决的问题。通过这个方法可以有效地确定支持行业标准的分布式总账所需的标准、基础设施和生态系统。

现行金融技术的风投融资环境，以及媒体对需要突破的下个行业的狂热报道，让创业厂商、合作企业和现有的企业纷至沓来，探索利用这一新技术的机会，许多金融机构正在私下试验使用可支持共识协议的技术来提供透明性。这恰恰与历史上的金融创新的历程，除行业要求或法规强制要求行业合作的少数情况外，如出一辙，但这样的历史重演将导致分布式总账同样陷入杂乱无章、各自为政的不连贯乱象。

整个行业应当把握该技术带来的机遇，评估如何升级改造，大幅降低风险和成本。DTCC十分熟悉这一流程，因为DTCC本身也是40多年前面对无纸化技术革命，行业合作现代化升级的产物。DTCC是那一次行业协作的产物，不偏不倚地关注降低整个金融行业的风险，拥有独特的优势。这是建立一个全行业计划，开发正确的架构，确定基础设施的要素重点，支持有重点的协作式试验，促进该技术成熟的机会。



