分布式账本技术白皮书

2016年11月11日

本书由麻双豹于2016年11月12日至11月19日翻译于华政
转发请注明出处。另：由于时间紧迫，错误与不足之处
在所难免，如您发现错误或有更好的翻译，请不吝赐教
联系方式：15821985389 译者身份：华政法律翻译硕士

Commissioned by

HONG KONG MONETARY AUTHORITY
香港金融管理局

1. 前言

对许多人而言，“金融科技”只不过是一个与他们通过智能手机应用程序或在银行的虚拟柜台使用的时尚银行或支付服务相关的术语。网上银行和移动支付应用程序是金融科技应用的重要领域，但它们绝不是唯一的应用领域。其他技术，从人工智能到大数据分析再到虚拟现实，每天都在推动金融科技的可能前沿的出现。这些技术可能给银行和支付服务带来巨大变革。本报告的主题 - 分布式账本技术（DLT） - 只是这一切刚开始发生的其中一个典型例子。

分布式账本技术，更通俗的说法是“区块链”。 它本质上是一种可以帮助参与者能够以安全有效的方式创建、传播和存储信息数据库技术。虽然数据库技术不是新的技术，但DLT的特别之处在于，在没有每个参与者都知道和信任的中心方来控制和管理的情况下，这些数据库网络可以顺利、安全地运行。

金融科技行业以及许多中央银行和监管机构很快发现，区块链的潜在应用并不仅限于买卖虚拟货币或商品。区块链技术允许网络参与者传送和更新信息或记录，并且这种传送和更新的方式是可信赖的、安全的和也是有效的，因而具有巨大的发展潜力。然而，虽然区块链技术的价值定位逐渐得到肯定，但在金融服务中使用区块链技术也带来了新的风险，引发了新的法律和治理问题。只有深入研究解决这些问题才能真正实现其全部潜力。作为监管机构，我们需要对区块链技术相关的治理、风险管理和法律问题有一个透彻的了解，才能促进分布式账本更广泛的使用。

研究白皮书

就此，香港金融管理局的金融技术促进办事处已委托香港应用科技研究院（应科院）进行一项关于区块链技术问题的研究计划。该项目的主要目标是对技术进行开放的深入审查（包括调查其潜力、风险和对监管的影响）；并通过参与概念证明工作来确定区块链应用于银行服务业的可能性。

本白皮书可视为这个更大型研究项目的第一阶段，旨在为香港的金融科技行业提供一个合理全面的研究，探讨区块链技术的主要特点、优点、风险和潜力。还包括在三个领域中对区块链技术应用进行概念验证工作的初步结果：抵押贷款申请、贸易融资和数字身份管理。该项目的下一阶段将提供概念验证工作的更详细的研究结果，以及关于这些工作是否可以付诸行动的讨论。还将解决区块链对监管的影响，以及银行和支付行业中区块链的一般控制原则。我们计划在2017年下半年以另一份白皮书的形式提供下一组结果。

本白皮书的问世离不开许多人的辛勤努力。香港应用科技研究院 （ASTRI）的专家作为作者和项目经理发挥了关键作用。我还特别感谢许多行业专家，他们提供了专题文章，讨论了关于使用分布式账本技术的非常具体和相关的问题。我很感谢银行及其他业界人士的积极参与，包括汇丰银行、渣打银行、中国银行（香港）、恒生银行及东亚银行的努力。他们提供了极其有益的帮助，慷慨地分享他们关于在业务使用分布式账本技术的的经验、见解和诚实度评估。

我相信，所有这些努力，不但会使这项研究计划对世界各地就分布式账本技术的未来发展所进行的辩论作出独特的贡献，而且亦会为金管局和本港银行界如何最好地把这项技术使用打下夯实的基础。

作者： Howard Lee

作者职务：高级执行总监

作者单位：香港金融监管局

2. 执行摘要

金融技术（Fintech）是一个金融业术语，通常是指新兴数字技术，据说会颠覆传统银行模式，为金融服务消费者带来更多便利并提高效率，有利于降低风险和降低金融服务提供商的运营成本。包括伦敦、纽约、香港和新加坡在内的一些主要金融市场试图建立一个可持续的金融技术生态系统，吸引金融技术人才，保持其竞争力。

为支持金融科技业的发展，维持香港作为主要国际金融中心的地位，香港金融管理局（金管局）于二零一六年三月成立金融科便利化办公室（FFO）。FFO的任务是启动银行和支付行业研究，进而推动新的金融技术的潜在应用的发展，而这可能对银行和支付服务的变化发展产生重大影响。

2.1 本白皮书的目的

在这个背景下，金管局通过FFO委托香港应用科技研究院（ASTRI）进行一项关于金融科技主题分布式账本技术（DLT）的研究项目，其中众所周知的例子就是“区块链”。 该项目的一个主要目标是对该技术进行无先入之见的深入研究，并确定其潜力和风险。本白皮书是本研究项目的第一个研究成果。其目的是为香港的金融科技业提供一个有关分布式账本技术的关键特征、优点、潜力和风险的综合研究。

2.2 分布式账本技术

分布式账本技术建立在一系列数据库网络上，允许参与者有效、安全地创建、传播和存储信息。这些数据库网络不需要任何每个参与方都知道和信任的中心方或中心管理员可以顺畅、安全地操作。同时，通过这些网络可以持续地对信息从开始创建时起的完整审计进行检测跟踪。此外，在未授权的情况下改变信息及其历史，即使不是完全不可能，也是非常困难的。换句话说，分布式账本技术操作设计为使得通过网络存储和传送的信息具有高度的可信赖性，并且网络中的每个参与者可以同时访问信息的公共视图。

在结构上，区块链可被认为是牢固链接在一起的一系列信息区块。任何给定的资产数字记录，无论是实实在在的房产还是虚拟商品的所有权契约的副本，都可以存储在区块中。当参与者创建一条新信息或改变关于资产的现有信息时，例如通过输入交易记录、状态改变、新市场价格或新所有者时，都会形成新的区块。在第一个区块之后新形成的所有区块被安全地添加到前一区块中，确保它们的真实性并且创建可信赖的审计跟踪。事实上，分布式账本技术的早期使用之一是在虚拟商品（例如比特币）领域，这些虚拟商品所有权的变化会被记录在区块链中。

分布式账本技术的设计显然优于某些传统技术。然而，如果不充分考虑到治理、部署、风险管理和合规性问题以及法律影响（如下所述），这种不断发展的技术也会带来风险。

2.3 治理

尽管采用了去中心化方法，分布式账本技术仍然需要一套所有参与者都必须遵守的通用规则以确保其准确性和可信度。当需要对规则进行修改或更新时，去中心化模式会带来一些挑战，因为这些修改需要得到所有参与方的同意和接受，确保分布式账本能够一致地运行。

因此，治理框架对于分布式账本技术的实施和持续运营很重要。该框架需要考虑监督和监控功能、规则设置，以及接受和变更控制管理。

2.4 DLT 平台

分布式账本技术平台主要分为两种：无中心的分布式账本平台和有中心的分布式账本平台。前者由公共节点维护，任何人都可以访问。比特币是一个众所周知的无中心的分布式账本平台的例子。它自2008年以来一直作为数字资产和支付系统存在，其使用大大加快了分布式账本技术平台设计的发展。后一种类型，例如Corda平台，仅涉及授权节点，因此有利于更快、更安全和更具成本效益的交易的实现。每个类别中的分布式账本技术平台都有自己特点。有些平台是为特定类型的应用程序专门设计的，另一些平台则用于一般用途。例如，在Corda中共享个人账本数据仅限于具有合法需要知道的各方，而在其他平台上并非如此。

2.5 部署

新技术取得成功的能力取决于它是否可以落地。分布式账本技术更适合应用于哪类金融服务，受到交易处理、交易验证和欺诈检测所需的性能和计算资源的影响。此外，为确保不同分布式账本技术网络之间、同一分布式账本技术网络内的帐本和其他非分布式账本系统之间实现互操作性所需的努力不应被低估，在进行配置之前也应仔细考虑。

2.6 风险管理和法律遵循

任何新技术的出现都不可避免地会带来新风险，分布式账本技术也不例外。即使参与者拥有的资产受到参与者数字证书的保护，没有正确的数字签名就不能更改信息，但某些传统的网络安全问题仍然会对分布式账本技术构成威胁。例如，拒绝访问攻击和其他网络攻击仍然可能针对分布式账本技术发起，导致其无法进行操作。

由于某些分布式账本技术应用程序（特别是比特币）的参与者是匿名的，分布式账本技术可能会被用来洗钱和销售非法货物，并且也可能被黑客用于进行勒索付款。虽然当在“有中心的”网络（其中只有授权和认证的参与者可以加入）中实现分布式账本技术时，这些问题可以在很大程度上得到解决，但是这种解决方案仍有待进一步研究。

不管分布式账本技术平台是否以“有中心”模式操作，当有关个人的信息存储在分布式账本技术平台中时，都存在个人数据隐私问题，而这个问题必须要解决。例如，由于存储在分布式账本中的信息一旦被添加就不能被改变或删除，任何应用程序均需要处理好如何既坚守数据保护的准确性原则又能确保个人校正数据的权利。此外，一些分布式账本应用可以跨越各个管辖区实施，而没有单个实体负责其运行，因此也需要解决与跨境数据流、法律可执行性、法律责任、争议解决，显示证据以及在境外的效力问题。

虽然在这一阶段，本白皮书的重点不是探讨所有这些复杂的法律和监管问题，但本文件确明确了这些潜在问题，并呼吁在这个研究项目的下一阶段进一步研究，我们也会邀请来自法律界的专业人士对这些问题进行研究。

2.7 潜在应用

金融科技行业和许多中央银行和监管机构认为，分布式账本技术能够广泛应用于许多银行和支付服务（如加密货币、交易后结算、记录查询和管理以及跨境资金转移）。分布式账本技术允许信息或记录由网络的参与者（其可以是彼此完全陌生的人）转移和更新，并且这种转移是高度可信赖的、安全的和有效的，因而具有巨大的潜力。在现有流程中，重要信息的传输和存储需要保证高度的安全，且在当前背景下这种传输和存储主要是人工的、依靠劳动力的、纸质的，而分布式账本技术有望替代现有的流程，从这一点上讲，该技术似乎更具吸引力。

2.8 概念证明工作

在编写本白皮书期间，一些银行业和业内人士通过在金融业的实践中利用分布式账本技术，通过自身实践更加深入的参与到概念证明工作之中。在现阶段，分布式账本技术已在以下三个领域发挥了重要作用：

1. 按揭贷款申请：银行为了做出良好的信贷决策，需要快速准确的对资产进行估值。 然而，银行、律师事务所和评估机构之间的沟通，在很大程度上，仍以纸质方式为基础，在沟通的过程中（有时）易于出错。 因此，把这些参与者连接起来的分布式账本技术网络可能对这有所帮助，例如他们可以据此自信地分享数字化评估报告和法律文件的副本甚至转移所有权，进而减少交易的时间和成本。

2. 贸易融资：这是另一个涉及纸张密集型流程的重要银行业务。分布式账本技术使用数字化文档，有望提高工作流程的效率和准确度，使整个交易历史及其附属信息更加透明。更重要的是，它可以降低通过使用伪造文件和双重或多重发票的方式进行欺诈的风险。z z

3. 数字身份管理：在现有系统流程中，为了确保法律合规而进行的“用户身份验证”（KYC）要求和客户身份验证流程，耗费了大量人力且需要来自银行的大量资源。此外，当前流程大量手工操作可能给客户带来不便，降低用户体验期望值。基于此，通过在分布式记账技术网络上执行概念证明工作来尝试通过自动化数字身份管理平台满足KYC要求和客户身份验证流程。

这种概念证明工作在不同领域的进程也不一致。最成功的是抵押贷款申请工作，目前以进入测试阶段。关于抵押贷款申请概念证明工作的更多细节，包括对详细的操作模式和有待解决的问题的讨论，将在本白皮书后面章节给出。

2.9 其他参考资料

本白皮书吸收了来自学术界和业界的专家意见，他们对分布式账本技术及其应用相关的潜在益处和挑战提供了一系列不同的细节和观点。

2.10 未来走向

对概念证明工作更深入的研究结果以及关于这些证明工作是否可以付诸实践的讨论将是本项目下一阶段的重点，计划在2017年下半年发布的另一份白皮书中呈现。第二份白皮书还将涵盖分布式账本技术对监管的影响，并探讨银行和支付行业分布式账本技术的一般控制原则。

最终，希望本白皮书对您更好的了解分布式账本技术及其潜在应用如何能够使客户和银行受益方面提供帮助。通过提供更好的金融服务和银行，为客户提供更安全、更高质、更高效的服务。 这反过来又有助于维持和改善香港银行和金融业的稳定性。

3. 分布式账本技术简介

分布式账本技术是用于构建可复制和共享账本记录系统的协议。该系统可以用于记录大量的事项，诸如资产所有权、资产转让交易和合同协议。虽然其账本功能类似于传统的基于纸张或基于电子的账本系统，但其功能更加先进。因为它提供了一种构建安全记录系统的新方法，为利益相关者提供更多透明度，并鼓励成员共同协作增强透明度。

分布式账本技术随着比特币的流行而受到关注。比特币是分布式账本技术最知名的应用之一，最早由匿名为中本聪（Satoshi Nakamoto）的人推出。比特币是一种数字资产，用户利用P2P支付系统可以直接进行交易，不再需要一个中心化的控制和管理系统。所有交易都需要由网络节点进行验证，并记录在全球级的分布式数据库中。

在传统上，支付业务需要作为中介（例如银行或清算中心）的中心化管理机构来证明付款人或付款银行具有足够的钱，以及处理货币及其在不同帐户之间的转让。与这些常规交易不同，比特币将分布式账本技术的维护责任分配给整个网络。只要验证节点能验证交易并将其发布到帐本，每次交易都将被添加到分布式数据库，并使其状态显示为已验证。因此，不需要中心化的机构来管理、控制或授权参与者之间的交易。

3.1 基本概念和操作模式

I. 什么是“账本”?

根据牛津词典的解释，账本是“一种金融项目账簿或财务账户的其它集合”。 账本已经存在了数千年，刚开始用语交易货物和服务，并需要保留交易记录。今天，传统的账本系统通常是一种在组织的信息系统基础结构内进行维护的中心化系统。

大多数人熟悉的现代“账本”的一个例子是银行往来账记录，这个账本保留了银行客户的每次借记或信用交易。重要的是，银行客户相信银行有能力安全地保留他们的银行记录（即账本中的银行帐户信息）。

II. 什么是“分布式账本”?

与传统的账本系统不同，“分布式账本”系统由该系统的所有参与者而不是由一个中心方（例如银行或清算中心）进行维护。每个参与者都是分布式账本系统的“节点”。从部分上来说，节点是单个参与者的计算机，每个节点包含一组完整的交易记录。从全局来说，节点参与建立和维护分布式账本。由于在每个节点中（而不是由某一方集中控制和管理）都能够维护和开发相同账本的“本地”副本，因此该系统被称为“分布式”账本系统。

(a) 如何更新分布式帐本?

与传统账本类似，每当交易发生时，分布式账本都会更新。然而，交易信息是在节点之间（例如，在两个系统参与者之间）交换，并且被添加为新的账本条目，而不是重写之前的记录（如在传统分类帐中）。

在没有可信任中心方的情况下，更新分布式账本的过程依赖于关于添加到账本的所有新信息的节点之间实现共识（或“分布式共识”）的过程。实现“分布式共识”又要求发生两个重要的过程：对每项交易的验证，以及将验证结果在分布式账本的所有其他节点进行“广播”。

- “验证” - 节点共同确定交易区块中的新条目是否有效，以及交易区块是否可以被允许进入账本。 具体来说，参与者（节点）需要对区块中的每项交易进行验证，以确保其内容是合法的。例如，必须对交易中发件人是否为正在售出资产的真正所有者进行验证。对于包含合同执行指令的交易，验证节点还将执行已由共识机制接收和确认的指令。

- “广播和共识” - 这是使验证节点能够在分布式分类帐中实现与新条目的一致的过程，它在验证节点已经验证一个或多个交易并启动将它们添加到账本的程序时开始。 验证节点首先向其他验证节点广播关于新区块的信息。 其他验证节点也可以验证相同的集合或不同的交易集合，但是共识机制允许它们在其本身之间进行通信并且商定要添加到账本的公共验证交易集合。

(b) 挖矿— 在验证过程中重要而又高消耗的任务

如上所述，需要以分布式账本的“开放”形式实现分布式的一致性，即任何人都可以将交易添加到账本里，并且没有人可以要求其作为中心信任机构对账本进行控制（通常称为“无中心分布式账本”或“去中心分布式账本”）。

实现上述目的的一条重要的途径是进行“工作证明挖掘”。该过程涉及所有验证节点，需要消耗大量的电脑运算能力。用以解决计算问题的第一个节点，也有助于建立一个交易区块。

然而，“挖矿”过程至少面临两个问题：

- 首先，挖矿过程需要消耗大量计算资源来执行计算。因此，参与者需要制定激励措施作为对参与挖矿活动以及最终维护账本所需的资源的投资。（以比特币为例，解决算法问题（并因此成功建立一个交易区块）的第一个节点的奖励是一定数量的比特币的。）

- 第二，挖矿过程通常需要时间解决复杂的问题。当验证节点对已验证的一组交易进行计算并试图将它们添加到区块时，不能同时对另一组新交易进行处理并将其加入到另一个新区块中。从这个角度说，挖掘过程会减慢交易处理速度。

(c) 用中心第三方塑造分布式账本

针对在无中心账本挖矿过程中产生的问题，已经开发了另一种类型的分布式账本。

通常被称为“有中心的”账本或“私有账本”可以由中心信任方或者联盟群体参与者拥有、控制和管理。只有被信任或已被审查的参与者才能对有中心的账本进行控制和维护。与账本相同的分布式副本由所有参与者保存。经注册或授权的参与者对账本共享有更强的控制力，可以跟踪资产所有权、机密文档的移动、清算状态及其他交易的行业级记录系统。

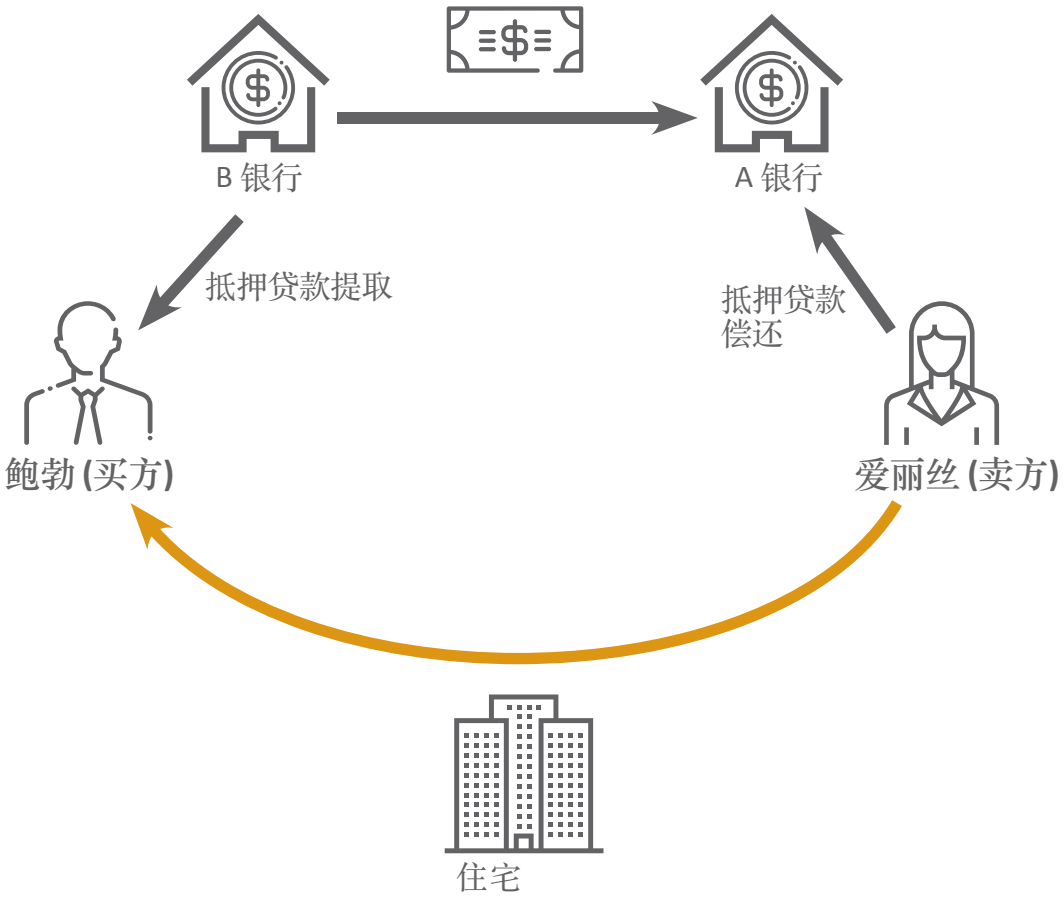
有中心的账本与无中心的账本相比，一个重要优势在于，验证过程不涉及计算密集的挖掘过程，不需要消耗大量的电能和计算资源。验证节点只需简单地检查交易是否有效，而不需要执行挖掘任务。这意味着账本的更新方式更快且更节能。如果只有受信任的参与者享有账本管理权限，且能够减少劳动力需求和减少重复，有中心的分布式账本受到网络攻击、出现安全漏洞的风险及操作成本（例如，需要较少的计算资源）也会较低。

3.2 详细步骤图

基于传统中心化数据库或系统中的交易

为了更好地理解分布式账本技术网络的特性，我们接下来将会对该技术网络处理房产交易（包括交易之后的产权变更）的潜在应用进行一些解释，包括随后的财产权利变更。

假设爱丽丝以1千万港元的价格将一个公寓卖给鲍勃。发生产权变更的关键事件如下：在签订买卖协议后，鲍勃从B银行获得抵押贷款。B银行然后在约定日期代表鲍勃将资金转移到A银行 。此后，该房产的所有权变更便会提交至土地注册处进行注册。



房产交易

现实生活的例子会涉及更多的当事人，例如需要一名鉴定人在鲍勃获得抵押贷款之前，向B银行提供房产价值评估，以及需要一名律师处理所有法律文件。

因此，上述例子只是一个简单但典型的产权交易，其基于对可靠的中心管理机构的信任，特别是政府部门向我们保证财产的合法所有权已被转让，而银行则确认我们的资金已经转移到指定帐户。

分布式账本技术提供了一种透明和共识机制来作为建立信任的一种替代方式，参与者通过参与合作共识过程来构建分布式账本，并记录和验证账本中的每个条目。

如何在分布式账本中完成交易工作?

现在，有关该房产的交易资料及其他有关资料被土地注册处全部存储在常规的中心化的数据库中，可以由不同方（例如，爱丽丝，鲍勃和银行）付费访问。

将来，该过程可能在分布式账本技术网络中发生，该技术网络旨在跟踪资产所有权权属，并且该技术网络会存储关于该公寓的交易数据和其他相关信息。

为了保持简单，我们假设使用有中心的分布式账本技术网络，因为只有有限的受信任参与者能加入这样的网络（例如土地注册处和银行）。在这样的网络中，这些参与者将成为节点。

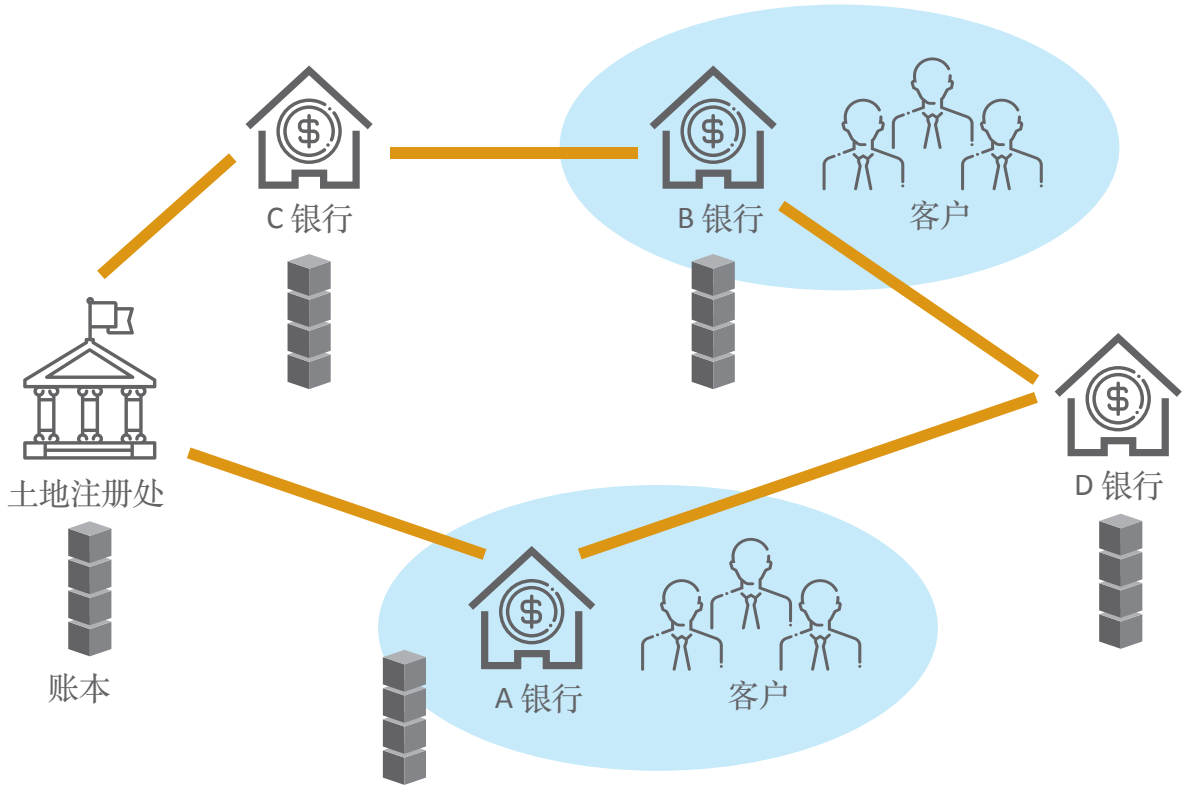
A银行（作为节点）将创建一项包含一组信息（例如，爱丽丝和鲍勃的个人详细信息、交易日期、地址和房产价格）的交易记录以及卖方的数字签名 （签署电子记录时需要）。

数字签名对于交易至关重要。它是一种用于证明交易中发件人的真实性和信息的完整性这两个核心要素的数学方案。这里使用的技术是非对称加密技术，其提供用于创建和发送交易所需的安全级别。 这个概念将在第四章进一步讨论。

交易广播和网络节点验证

A银行向所有其他节点（即土地注册处和其他参与银行）广播交易（附有签名），使得交易可以由它们中的任何一个进行验证。

由于每个节点拥有一组完整的关于房产的历史交易数据记录账本的本地副本，所以节点能够查看其自己的链和对检查交易的有效性（即确定爱丽丝真正拥有房产所有权）的历史进行记录。



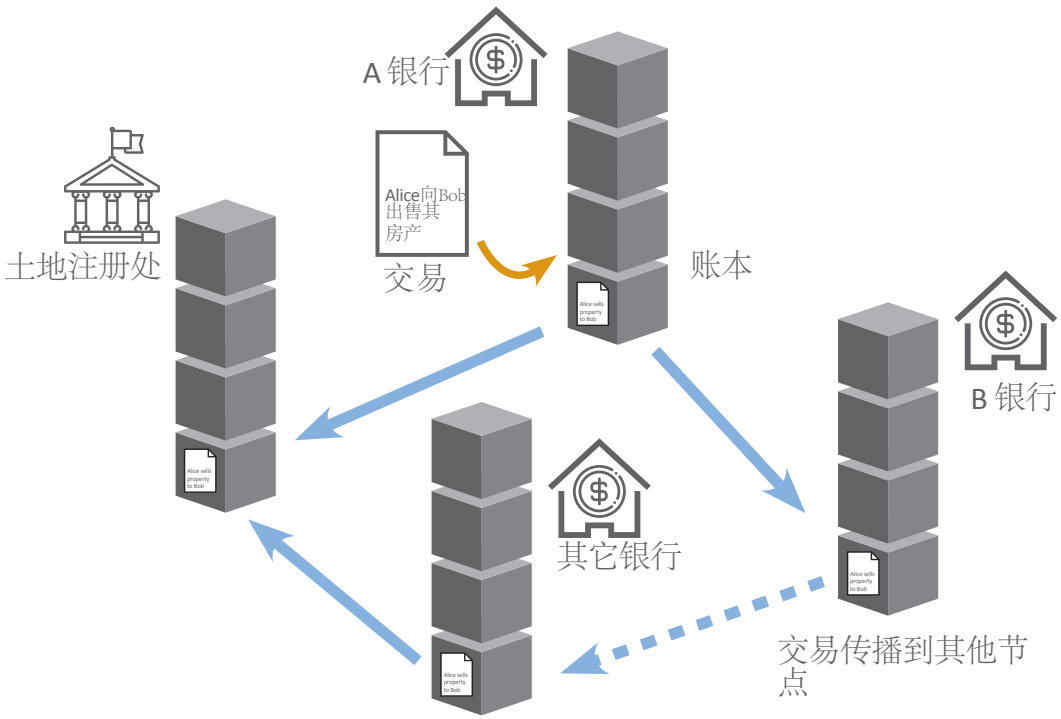
土地注册处及注册银行维护其可复制账本副本的分布式账本技术系统

当该特定事务由DLT网络的节点验证时，很可能会有其他交易同时发生。例如，Cathy可能从David购买房产，并通过C银行向D银行结算付款。

然后节点将所有尚未记录的包括由爱丽丝达成的交易在内的新创建的交易分组到有中心的账本，并将这些交易编译为“交易区块”。

新交易区块

一旦交易区块已由验证节点编译，则验证节点就会将该交易区块广播到分布式账本技术网络内的所有其它节点。其他验证节点也可以对相同的一组或不同的一组交易进行验证，并且共识过程允许它们在其自身之间进行通信，并且对要添加到账本的一组公共验证交易达成共识。 然后，依此类推。



在该分布式账本系统中，A银行将“爱丽丝向Bob出售其房产”交易发送至其它节点，然后其它节点再将该交易添加到其账本的副本。

现金付款的结算

付款怎么办？ 这取决于分布账本络技术网络的设计。

由于分布账本络技术网络只是一个包含数据记录的分布式账本系统，因此不会转让任何实际资产，只有新的记录或条目不断被添加到分布式账本系统网络。因此，可以在分布式账本技术网络之外（即，通过单独的支付系统）或通过相同的分布式账本技术网络来结算用于财产交易的款项。在后一种情况下，支付过程将被记录为参与者之间的数字货币活动。换句话说，产权转让和相关付款行为理论上可以在“交付与付款”的基础上实时完成。

3.3 颠覆财产

分布式账本技术的防篡改性

众所周知的分布式账本系统的防篡改性有助于在参与者之间建立关于系统完整性的信任。其防篡改性通过两个元素实现：验证系统和加密技术。

从概念上讲，分布式账本技术是区块组成的链。每个区块包含一组称为交易的条目。通过验证节点将新条目收集到新区块中，然后将新区块添加到链中。当收集更多的新条目时，创建更多的区块，链的长度也会随之增长。

分布式账本技术可以保证这个链被篡改的难度会很大。图谋不轨者若试图对链做任何修改，都需要提供证实修改真实性的证据。而生成这样的证明需要执行冗长的加密操作，并要付出高昂的成本。此外，捏造的证据很容易被分布式账本技术网络内的其他验证节点检测出来。

链中的区块通过使用哈希函数构建的链接连接在一起。区块的链接与其内容整体相关。任何试图改变链中区块内容的做法都会导致其哈希链接的值发生变化。这就打破链的整体性，剩余的链比原来的短得多。这种情况很容易被其他参与者立即检测到，其他参与者将永远拒绝改变这些链并继续使用原始链。

哈希函数是一种单向数学函数，将数据转换为称为哈希的一系列随机字符。对数据的改变，无论多么微小，都会大幅度地改变哈希。 此时再想从哈希中导出原始数据已经不可能了。

分布式账本技术的不可更改性和透明性

分布式账本系统是透明的，因为所有交易都是公开的、可追踪的，并永久存储在分布式账本技术网络中。虽然私有的分布式账本技术网络可以对交易添加访问限制，但是它保留了对利益相关者对其公共交易具有公共访问权限的特征。

当任何人开始在分布式账本技术系统上交易时，所有的交易历史开始被记录在系统中。这种历史是永久记录、不可改变的，并且可供公众或利益相关者访问。这种高透明度和高可靠性是建立对网络完整性的信任的重要因素。

3.4 智能合约

随着技术的发展，“智能合约”逐步出现，为分布式账本技术增加了更多的应用领域。参与者被允许写入自行起草的协议（即智能合约），并将其嵌入到分布式账本技术网络的记录中。此类合同是以计算机代码开发的，使分布式账本技术能够在严格遵守合同条款的情况下自动执行。可以将触发事件设计和构建到智能合约中，以在发生指定事件或接收到某些数据时激活某些行为。典型的示例就是在到达指定日期时触发支付。

这项研究确定了一些可能的子用例的概念验证工作，智能合同概念将包括在这些子用例中，以帮助我们更好地了解智能合同的潜力。

3.5 本章小结

基于本章中阐述的关键优势，分布式账本技术系统显然有可能为银行和支付行业创造新的机会、并提高效率，包括在分布式系统中建立信任，快速、安全广播信息，实现记录和交易的完全可追溯性，降低运营成本以及弹性大。　然而，在做出分布式账本技术是所有银行和支付问题的最佳解决方案的结论之前，需要做更多的工作来确定现有分布式账本技术是否成熟，是否足以满足金融界的要求，并确定分布式账本技术需要纳入什么关键属性或要求以促进银行和支付行业广泛、自如的使用。

由于分布式账本技术仍在不断发展，更加新颖、更具创新的操作模式不断引入和测试。比如说，R3的Corda 分布式账本技术，它构建了一个分布式账本，而不使用区块链作为其构筑区块。诸如此类技术的研发就提供潜在操作模式而言，可能会有其它的分布式账本技术选择。

本文将继续检验分布式账本相关的技术，并确定与之相关的可能问题。 本文还将介绍子用例来演示分布式账本的潜力。

4. 技术

上一章对分布式账本技术进行了概述。本章旨在深入研究分布式账本的基础技术和安全设计。在分布式网络中，运用难以被诸如网络中诚信度较低的人或未被授权之人在未授权情况下对数据进行更改的方式来创建、传输和存储信息。其在保护信息完整性方面具有极强的稳健性，这是对齐宏观层面的顶层设计以及微观层面的在管理和传递信息时所采用的详细技术和具体安全安排。

接下来，我们将讨论分布式网络如何保护信息完整性： 首先从“宏观”的角度，对其一般设计进行讨论，然后在“微观”层面，对各种技术和安全安排如何在某些关键过程中发挥功效进行讨论。

4.1 通过设计保护信息完整性：“宏观”视角

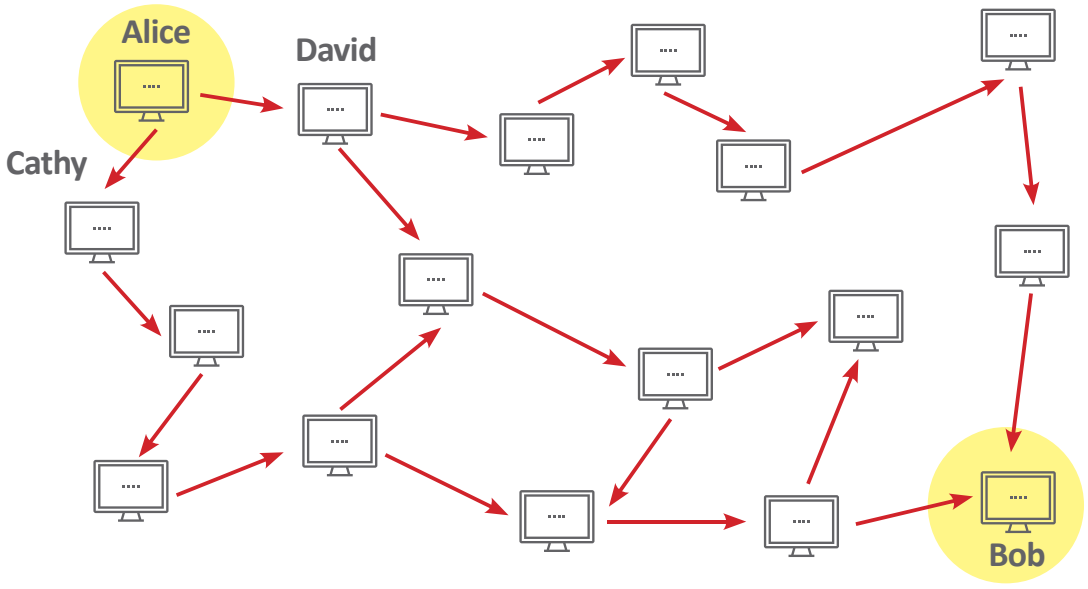
分布式账本实质上是一个去中心化的数据库，数据库中的信息在与网络中连接的多个位置中被复制。任一参与者都可管理和构建可复制的数据库副本。

这些参与者基于既定程序或“协议”积极地进行交流，通过（a）进行交易，（b）同意将交易添加到账本，并在添加交易顺序上达成一致。这些参与者称为“矿工”（在无中心的网络中）或“验证节点”（在有中心的网络中）。

分布式网络

参与者通过分布式网络彼此连接。参与者互联的常见方式是通过一种称为P2P的“点对点”网络。P2P网络是庞大的，能够覆盖到面积大的地理区域。每个连接的计算机称为“对等”节点。节点通过连接到其信息已被公开的、已为公众知晓的点来加入网络。然后，它通过从该节点接收的信息来了解其他对等。 同时，其他节点了解这个新节点。

P2P网络覆盖面广并且包括许多节点。单个节点连接到几个其他节点，而这些被连接点对等体本身也会连接到网络中的其他对等体。当对等体向他或她的对等体发送交易时，这些对等体将事务转发给其他对等体，然后其再次将其转发给其他对等体。最后，网络中的所有对等体接收与该事务相关的信息（参见下面的图示）。



点对点（P2P）网络示例

1. 节点连接到几个其他对等体，这些对等体再连接到其他对等体。
2. 如果Alice想要将一条消息发送至网络中的所有节点，她首先将它发送给她的直接对等体，即Cathy和David。
3. Cathy和David再把他们接收到的消息发送给他们的直接对等体。

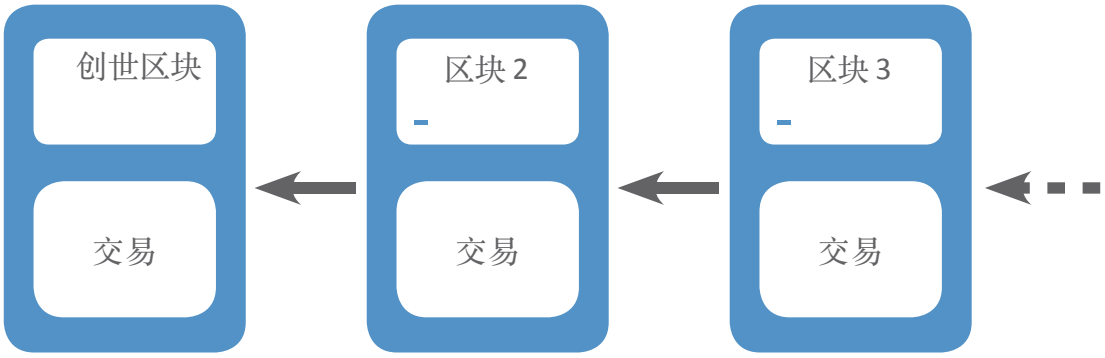
图示：P2P网络和数据包转发

区块链中的数据记录

账本记录了信息“区块”的链。每个区块包含一组交易。新一组交易会形成新区块，构成账本的一部分。因此，所有交易存储在该账本中，不能被篡改，该账本可在所有验证节点之间进行复制。

账本的第一个区块称为“创世区块”。下一个新区块添加到该块，就形成了区块链。随着更多的新块添加到该区块链，这个链就变得更长。每个区块具有唯一的标识符，并且通常由哈希值表示。每个区块指向其紧邻的上游块（参见下面简化的“区块链”图）。区块的位置根据其在分类帐中的位置来描述。

用于表示区块中一组交易的默克尔树增强了对交易的搜索和对块链的验证能力，因为每个块可以包含许多交易。详情请参阅技术说明（I）。



简化区块链构造

信息“区块”：创建和添加

矿工或验证节点的关键作用是收集新交易有关的信息，将此信息放入新的“交易块”，并将其添加到账本中。

分布式账本技术的一个重要特征是，向账本添加新交易的这个过程需要通过共识机制和验证机制，防止恶意添加虚假交易和虚假区块。

在无中心化的网络和有中心化的网络中的实现方式：

1. 无中心化网络

在无中心化的网络中，矿工必须在新区块上解决数学难题，然后才能将该块添加到帐本中。矿工的解决方案随后转发给其他矿工，其他矿工验证后，矿工们会将该方案添加至他们账本的副本中。

解决该难题的机制被称为“工作量证明”，这需要大量的计算资源来找到解决方案。这种资源可以根据功耗或硬件资源来理解，诸如物理存储器或专用硬件逻辑的大小。第一个成功解决这个问题的矿工会得到奖励，作为对他或她所做努力的回报。这种期望受到奖励的行为可能是该过程被称为“挖矿”以及与这个过程相关的人被称为“矿工”的原因。

如果不止一个矿工解决同一区块的数学问题，或者生成具有不同内容的区块，则可通过共识协议来解决差异，该协议是允许相关各方达成协议的一组规则。一旦达成协议的过程完成，只有达成共识的区块被添加到账本中，之后复制的网络账本副本会再次保持相同。

达成共识的过程也是为了防止不诚实的矿工添加包含恶意交易的区块。如果某一矿工试图通过非法地宣称对本不属于他的财产的占有的方式来改变交易历史，则矿工必须用包含虚假交易的区块替换账本中的区块。然而，这将需要矿工重新创建该块后面的其余块，否则他的账本将比当前的短，并且在共识过程中会被其他所有矿工自动拒绝。

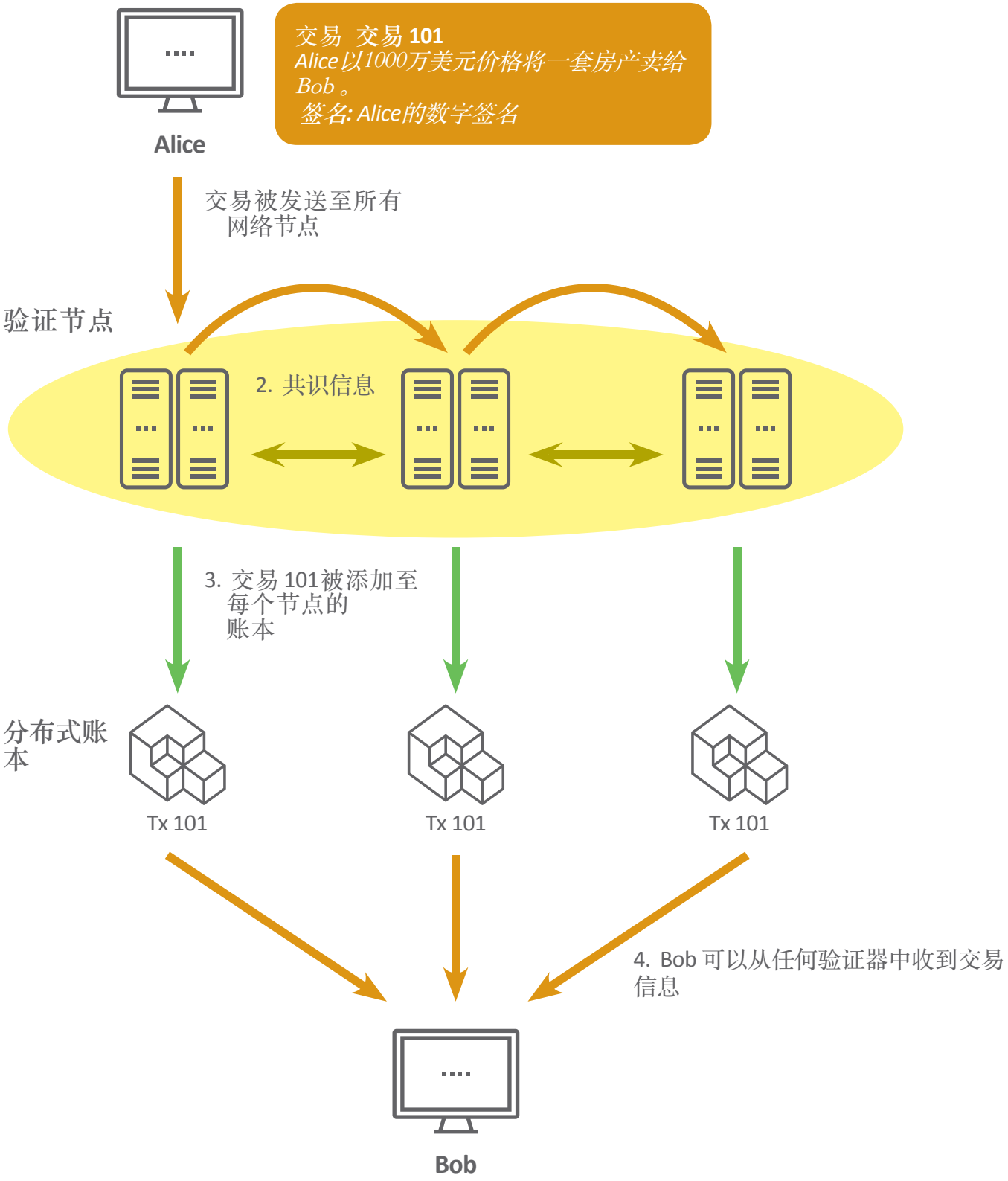
如上所述，如果矿工试图重新创建所有这样的块，他将不得不解决创建这些块所需的所有数学上的难题。而且，块之后的区块链越长，这个任务就越困难。鉴于所有矿工都在用大量的计算资源进行采矿，有时达到其最大能力的情况下，不诚实的矿工很难（如果不是不可能）做到这一点。

2. 有中心的网络

在有中心的网络中，验证节点是可信的，因此不需要解决数学上的难题。相反，他们只需要提供其可信任身份的证据，以便参与协商共识的过程。在共识过程期间，每个可信验证节点收集新交易并且与其他可信验证节点交换其对这些新交易的收集。一旦共识过程完成，所有可信验证节点都具有包含相同新交易集合的相同新块。

在生成新块之后，挖矿者/验证节点执行共识过程以确保所有节点都能看到相同的新块集合，并且还以相同的顺序将它们添加到分布式账本网络。因此，在添加新块和新交易之后，所有可复制副本仍保持相同。

在下面的图表中使用第三章中给出的属性事务的示例来说明分布式账本的技术设计。



示例：在该分布式账本技术网络中，Alice签署并发送以1000万美元价格将房产卖给Bob的合同。

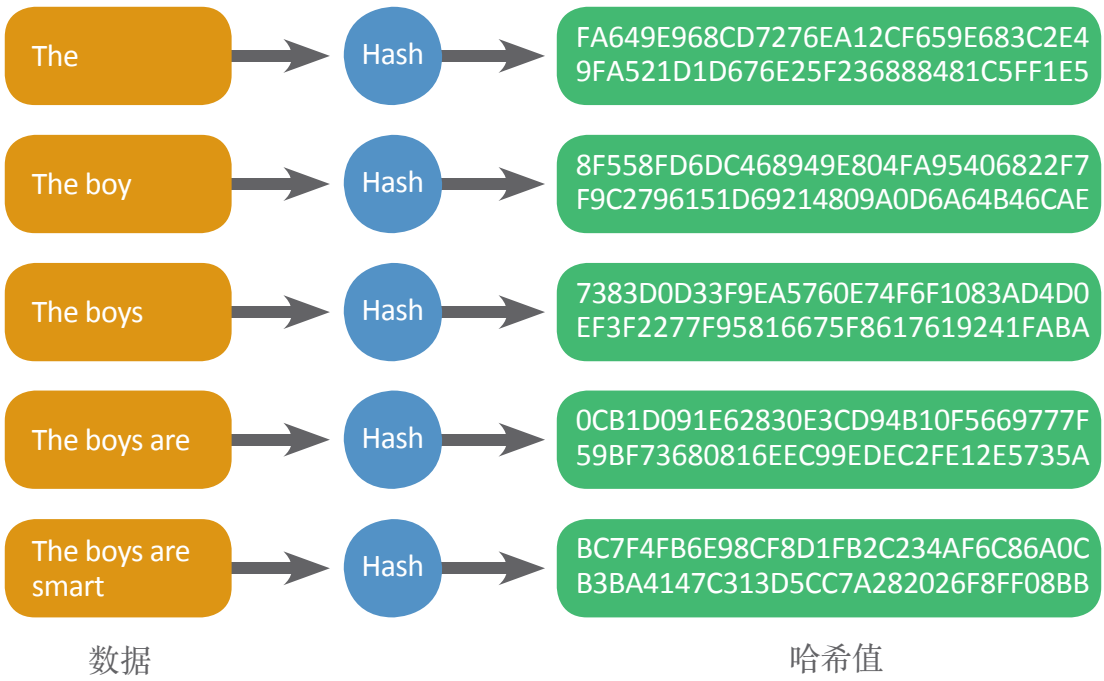
4.2 使用加密技术保护信息完整性：“微观”角度

分布式账本技术系统使用加密技术来保护账本数据：包括通过网络传输的数据和本地存储器中的数据。数据真实性和保密性是分布式账本的两个主要要求。

哈希

分布式账本技术账本包含大量的块和大量的交易数据。一旦块和交易数据已经存储在账本中，这些块和数据是不可变的，即不能被篡改。在宏观层面，验证节点之间的共识过程确保没有恶意验证节点能够将伪造的交易添加到分布式账本技术网络中。在微观层面，应用哈希技术来检测原始数据所发生的任何改变。这是一个数学单向函数，它将一条数据（无论其大小）汇总为“哈希值”，哈希值用作表示大量数据的固定大小的唯一值。对数据的任何更改都会导致其哈希值也发生更改。因此，为了检测数据是否发生变更，只需要在数据记录上运行哈希函数以获得哈希值即可，而不再必须检查冗长数据记录中的每条信息。如果哈希值已经改变，则可以断定数据记录已经被改变。

哈希函数的力量在于，任何人都几乎不可能预先确定哈希值，相应地，也不能创建生成预定哈希值的数据记录。原始数据记录的微小更改将导致哈希值的重大更改。在技　术世界有不同的哈希算法。一个常见的示例是SHA256，它将任何大小的数据字符串减少为256位数（请参见下面生成SHA256哈希的插图）。



不同字符串生成SHA256哈希的示例

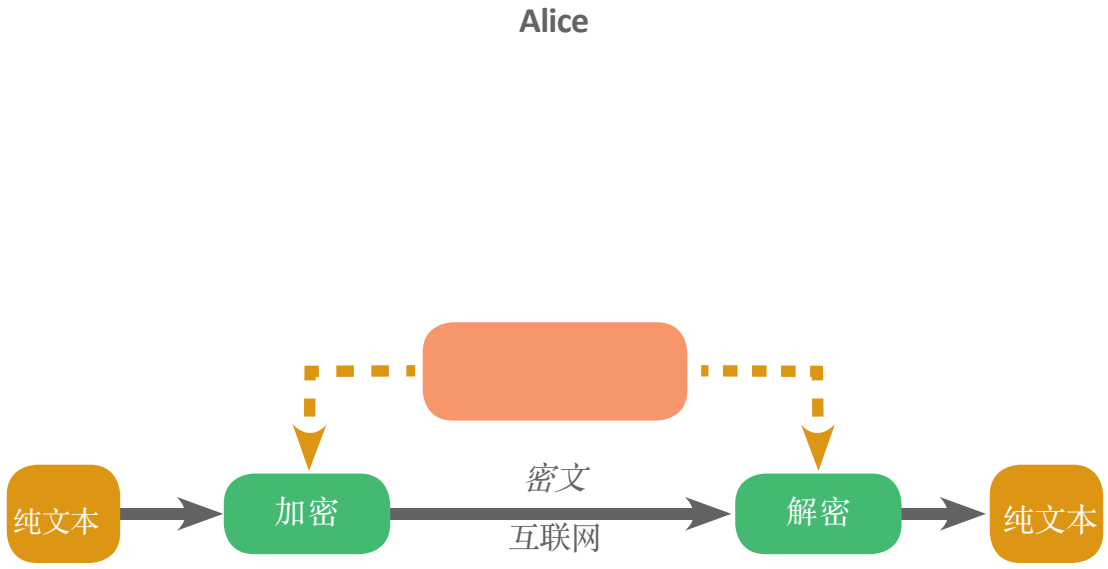
由于哈希运算将任意大的一条数据缩减到固定大小的唯一短数据串，所以它经常被用作数据本身的唯一标识符。同时，它保持数据的内容不被公开。唯一的ID不仅对于表示数据本身非常有用，还可以用于其他目的。比如说，在一些分布式账本应用中使用的存在证明。拥有包含机密信息的数字文档的人可以将文档的哈希值传递给第三方作为对文档的引用和证明其存在的证据。随后向第三方提供数字文档的副本时，该第三方可以通过验证哈希值来验证数字文档的真实性。

除了用于总结数据和检测数据是否发生改变之外，分布式账本技术进行创新，已将哈希函数应用于其它目的。无中心的分布式账本技术网络使用哈希函数来执行挖掘工作证明。当创建包含一组交易的新块时，矿工运行哈希运算的不定迭代次数。在每次迭代中，矿工选择一个称为nonce的唯一编号，将其与区块的内容组合，并对该组合进行哈希运算。然后，矿工检查所得到的哈希值是否与分布式账本网络指定的位组合模式匹配。如果不匹配，那意味着矿工没有找到合适的nonce数，因此必须使用新的nonce数开始另一轮哈希运算。当最终找到合适的nonce数时，矿工可以合法地声明已成功创建了新块，并且nonce数也可以作为证明来呈现。

挖矿过程需要大量计算，因为矿工需要在过程需要非常大的努力进行哈希运算，直到找到一个nonce，产生一个匹配的哈希值模式。无中心的分布式账本中的矿工相互竞争，希望自己第一个找到正确的nonce数。第一个找到正确nonce数的矿工通常会在分布式账本系统中受到奖励。技术读者可参考技术说明（II）的详细说明。

对称密钥加密

在对称密钥加密中，单个密钥用于加密和解密数据。这允许人们加密他或她的数据并防止他人知道其内容。只要他本人不向他人透露密钥，任何人都不能破解该数据。



图例: Alice使用对称密钥对数据进行加密解密

在上图中，使用对称密钥将明文加密为密文，然后可以通过诸如互联网的公共信道安全地发送密文。接收端使用相同的密钥将密文解密回纯文本。

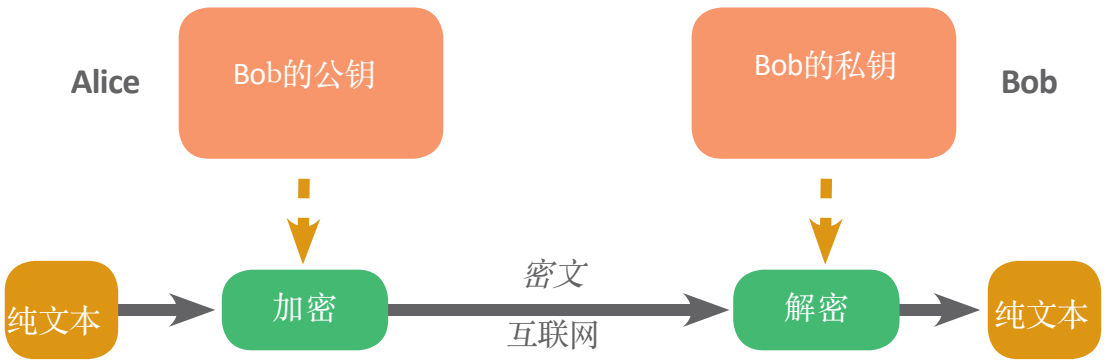
对称密钥加密的一个流行示例是高级加密标准（AES）。 AES的一个常见用法是用于在线交易和通信，在这两个领域中，AES保护通过公共网络进行交换数据的机密性。AES密钥长短不一，更长的密钥长度能提供更好的保护。更长的密钥长度也使得外人更难猜测。目前，许多安全的网上银行交易都受到AES加密保护。在每个网上银行会议期间，会设立新的AES密钥，这样在银行web服务器和客户端使用非对称密钥密码术彼此认证之后可加密后续网络通信。

非对称密钥加密

非对称密钥也通常用于数据加密。它允许不愿共享对称密钥的两方彼此发送密文。

在对称密钥加密中，相同的密钥可同时用于加密和解密，而与此不同，非对称密钥加密需要使用一对密钥：公钥和私钥。公钥用于加密数据，而私钥用于解密数据。例如，如果一个人想要使用非对称密钥密码术来保护他自己和其他人之间的数据交换，则可为此目的创建一对密钥（即，公钥和私钥）。然后将公钥发送给另一方，而私钥由有关人员保存。当第三方想要向此人发送数据时，第三方利用公钥来加密数据。由于接收者拥有私钥，所以他是唯一能够解密由第三方发送的加密数据的人（参见下图中的图示）。

非对称密钥加密的优点是，它允许两个陌生人在公共网络上交换机密数据，而不用担心数据的安全性，并且不需要共享单个密钥。



图例: Alice将使用 Bob 的公钥将加密数据传送给Bob

RSA公钥加密算法是最广泛使用的非对称密钥加密系统之一。其密钥长度通常采用2048bits长的密钥，并且长度会更长。它通常用于在客户端和受信任的服务器之间建立安全连接。一个示例是连接到银行web服务器的客户端，连接之后，机密数据可从客户端传输到银行的web服务器。客户端使用银行的公钥对数据进行加密，并将生成的密文发送到银行的Web服务器。在接收到密文时，银行的web服务器会对密文进行解密并将其转换为纯文本。加密数据在通过因特网传输期间，未授权的第三方若想截取这些加密数据，会发现对这些加密数据进行解密和访问都是困难的（如果不是完全不可能的）。

数字签名技术

数字签名基于非对称密钥加密技术，在分布式账本技术中用以证明交易的真实性，即，证明某个人人是指示的数字身份的真正所有者。当一个人创建和发送分布式账本交易时，该交易必须有该人的数字签名。

在数字签名技术中，人们创建一对密钥：公钥和私钥。创建者向公众释放公共密钥，同时对私人密钥进行严密、安全地保存起来。当该创建者向第三方发送交易时，使用私钥对交易的内容进行签名。然后，交易的接收者可以使用公钥来验证添加到机密交易的数字签名是否是该人的真实数字签名。任何人尝试使用不同的私钥签署交易会很容易被检测为假冒。

数字签名提供了用于在互联网上进行在线交易和发送经认证的数字文档的安全手段。例如，2015年香港银行机构推出了需要由付款人和银行的数字签名的电子支票业务，该电子支票可以通过公共网络发送，而不必担心未经授权方的篡改。同样，分布式账本技术使用数字签名来验证互联网中交易的真实性。

4.3 智能合约

智能合约具有分布式账本技术的特质，该合约在区块链分布式账本上执行。合约是多方之间的协议。合约条款由分布式账本技术的验证节点执行的计算机语言或代码进行规定。分布式账本技术的验证节点基于所指定的条款公平地执行智能合同。

典型的智能合约有以下四个主要组成部分：

- 合同条款 - 所有相关方商定的一组预先设定的条款和执行条件;
- 事件 - 一个或一系列可触发交易的特定事件，事件应在合同中详尽定义;
- 执行 - 触发交易时，合同签署方之间的价值转移;和
- 结算 - 在案资产和离岸资产的结算。

和传统合同一样，智能合同需要由相关各方共同起草。为了使分布式账本技术执行智能合约，合约条款可以规定执行条件，如收到各当事方的数字签名以及某些事件或条件的发生等。

分布式账本技术中智能合约的创建和执行不需要中介的参与。双方可以简单地将智能合约输入分布式账本技术网络，智能合约将根据其条款和条件执行。这带来了许多好处，包括快速和自动执行合约、降低交易成本，以及制定无二意性的合同条款。

智能合约可以用于许多目的，例如处理公正交易所、项目资金抵押、上市公司企业行动和投资者投票系统等事项。

智能合约的多方签字特征通常用于智能合约需要不同当事方的背书以达成交易之时。这意味着智能合约的条款需要明确所有需要签名者的身份，并且分布式账本技术网络只有当事各方已完成签名才会执行合约。非对称密钥加密用于实现多方签名的要求，智能合约通过规定所需签名者的公钥信息来明确所需的签名。或者，智能合约可以指定一组授权签名，并且同时规定触发执行合同所需的最少签名人数。

5. 部署

分布式账本技术若要实现简单高效的部署，就需要认真考虑这项新兴技术的不同特点。本章将会从性能和互操作性两个角度讨论分布式账本技术的平台部署。

5.1 性能

分布式账本技术的性能是决定分布式账本技术是否以及如何有效应用于不同金融服务的重要因素。在承载大量活动的应用中，例如资金转移系统、证券交易系统和后交易基础设施中，性能是成功关键因素。

可以在以下术语中评测分布式账本技术平台的性能。

a. 区块大小限制和区块生成频率

分布式账本技术网络的生产能力基于网络在给定时间段内可以处理交易的数量。交易处理包括验证交易并将其添加到分布式账本技术网络内的区块。分布式账本技术平台通常定期地生成区块。区块大小限制通常对区块可能承载的交易数量设置上限或限制。分布式账本技术网络可以通过增加区块生成的频率或通过提高块大小限制来寻求增加生产能力。

区块大小限制

由于各种原因，分布式账本技术平台对区块大小施加了限制。该限制在平台规则和策略中规定。

无中心的分布式账本技术网络的形成通常由一组开发者开始，通常是为分布式账本技术网络设置初始策略和规则的开发者。因为大多数时候这样的网络是开源的，所以其后的规则更新通常是公开的建议。这些建议，如果被该组开发人员接受，将被添加到管理分布式账本技术网络的规则集中。

对账本区块设置大小限制的分布式账本技术平台可以使用不同的参数来设定限制。

一些分布式账本技术平台直接根据其可容纳的最大字节数来设置块大小限制。其他平台不限制字节计数，而是使用其他参数。一旦达到由参数设置的目标，则其它的交易便不能再被添加到当前区块。此时，该区块会被即刻处理，验证并添加到分布式账本技术的账本。该类参数的例子包括交易的紧急程度或验证事务的计算开销。

例如，以太坊（Ethereum）是一个分布式账本技术的平台，通过规定最多允许的燃料数量限制区块的大小。交易处理消耗了一定量的燃料。每个以太坊区块都明确了对该块内所有交易可以消耗的燃料总量。该限制不是固定值，并且可以在区块之间改变；它是由矿工决定的。然而，以太坊对连续区块之间的燃料限制的允许变化率进行了控制。

区块生成频率

一些分布式账本技术平台为区块生成设置固定频率。其他的平台的区块生成时间则是可以变化的。

例如，比特币每10分钟产生一个区块，而以太坊目前以平均每13秒的时间生成一个区块。

有中心的分布式账本技术网络可以找到实现动态区块生成时间的原因。例如，紧急交易的存在可能需要立即验证并添加到账本中去。

b. 交易确认时间

这是指在分布式账本技术下，确认一项交易之前的必要时间延迟。如果交易信息已经被添加到账本内的区块中并且在整个分布式账本技术网络中的验证节点之间的共识过程已经存在至少一定量的时间时，则认为该交易已被确认。在将区块添加到分布式账本技术的账本之后，该区块的历史长度通常可以通过在其后添加的后续新区块的数量来测量。后面跟随的区块数量越多，以后不会被撤销的可能性越大。无中心的分布式账本技术网络通常具有较长的确认时间，因为共识过程（即挖掘的工作证明过程）需要较长的时间来进行。一些有中心的分布式账本技术网络通过应用特殊网络架构和共识算法来减少确认时间，这一方面减少了确认过程所需的时间，也降低了区块被撤销的风险。

多少区块确认才能将交易视为已确认?

当区块由验证节点创建并添加到帐本时，可能另一个验证节点几乎在同一时间已经创建了竞争块。由于验证节点通过P2P网络连接并会出现网络通信延迟，所以在两个验证节点要在一定时间段后才会出现冲突。如果一个区块胜出，则另个区块中的一些交易可能会被撤销。因此，在将区块添加到账本之后，建议交易方等待多个区块确认时间或挖掘周期，然后还要确保区块中交易的安全并且不会被撤销。在每个挖掘期间，验证节点运行新一轮的共识过程以确认向账本添加新区块。如果区块在多轮挖掘周期之后仍保持在帐本内，则这意味着在该延长的周期内验证节点没有检测到区块冲突。

关于设置性能的非技术性注意事项

看起来性能更高的分布式账本技术网络更受欢迎。然而，某些分布式账本技术平台却更喜欢将性能设置在某一水平之下。例如，处理本地加密货币的分布式账本技术平台上的区块产生速率与产生新币的速率直接相关，因为新币的可用性可能影响加密货币的价格。因此，这样的平台故意将区块生成速率保持在协议设定的限制之下。

关于验证节点计算能力的考虑

当分布式账本技术平台增加其区块大小或区块生成频率时，可以处理更多的交易。及时处理大量交易的负担落在了验证节点上。付款交易要求验证节点验证付款来源，而智能合约交易要求他们运行智能合约脚本。

无中心的分布式账本技术平台在规划提高其性能时需要考虑这一点。如果新性的能标准需要验证节点的计算能力显著增加，则分布式账本技术平台必须确保这不会推出许多较弱的验证器，并保证不会因此将验证活动留给几个强大的（并且可能不诚实的）验证器。如果这种情况发生，分布式账本技术网络将面临51％的风险，或不诚实的验证器占据多数而控制平台或中断其常规功能的风险。

确认时间和网络架构

分布式账本技术通常在P2P网络上运行，可以覆盖很广的区域。分布式账本技术系统包含由一组验证节点集中维护的可复制数据库。在验证器之间达成共识需要在分布式账本技术网络中的所有验证节点之间交换信息。然而，分组交换可能会出现网络延迟和偶尔中断。共识算法就是在考虑到这些问题后，提供可靠的交易确认方法。这对确认时间的长短有影响。如果确认时间段设置得太短，会增加了账本分支的机会（分布在节点中的账本的副本存在冲突的内容），会加大先前确认的交易出现未被确认或被撤销的可能。 P2P网络还可能会出现碎片化情况，网络的碎片与网络的其余部分分离暂时隔离。如果处理交易后，在分布式账本技术网络的不同碎片中的验证节点正在创建区块，则一旦分布式账本技术网络被完全恢复，这些节点需要协调它们的账本中的差异。

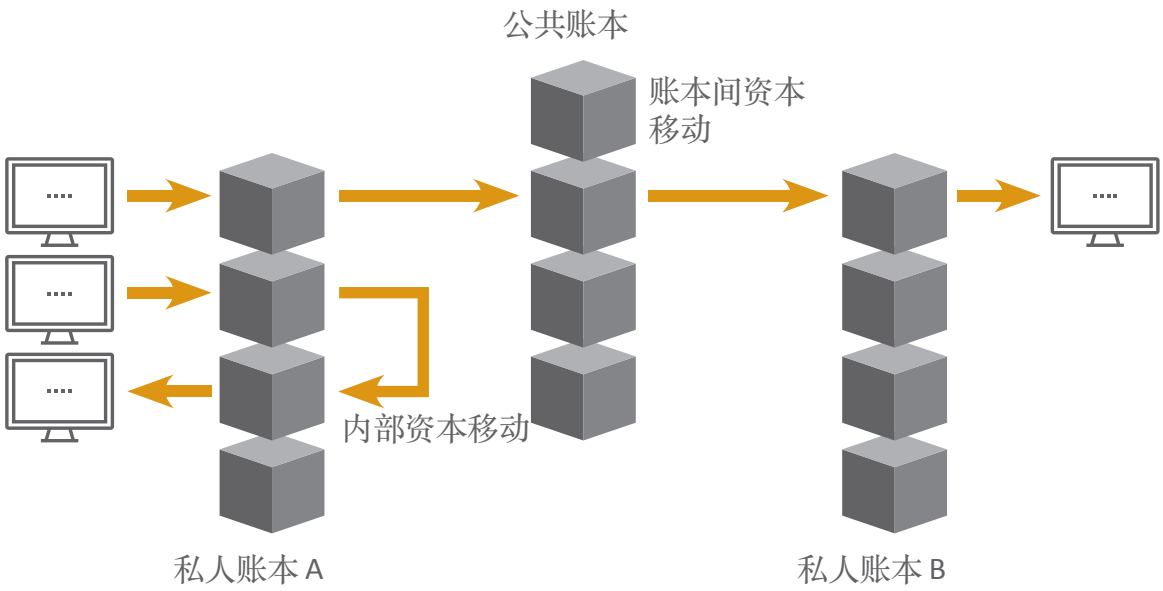
如果要提高性能，特别是在允许网络中，共识算法和网络架构都是要考虑的要素。然而，虽然确认时间可能需要比中心化数据库所需的时间更长，但是分布式账本技术网络提供了其它特征，并在其他方面提高了效率，这也是其魅力之在。

5.2 互操作性

分布式账本技术网络之间的互操作性

分布式账本技术平台通常运行在自己的网络域中。分布式账本技术平台是为了解决在他们支持的应用程序中出现的不同问题。随着分布式账本技术网络越来越广泛的应用，且应用方式也出现多样化，新的分布式账本技术平台的数量也在不断增加。最新的两个例子是Corda3和超级账本4。每个都有自己的独特特性，如独特的共识算法和专为不同应用程序设计的功能。

目前，一种称为“楔入式侧链”的技术使多个账本能够同时运行，并且资产可以在不同的分布式账本技术的账本和平台之间转移。随着更多具有不同特性的该类账本强强联合，不同的分布式账本技术网络的全球生态学也正在形成。将不同分布式账本技术的账本连接在一起，并在它们之间传输资产，会产生新的技术和安全挑战。技术必须使分布式账本技术的账本能够清洁、顺畅地相互连接。每个分布式账本技术的帐本还需要确保其相邻账本中的任何不当行为不会通过界面移动并影响到它。



账本内（a）或账本间（b）资本移动图示

改变分布式账本技术策略，创建新的账本

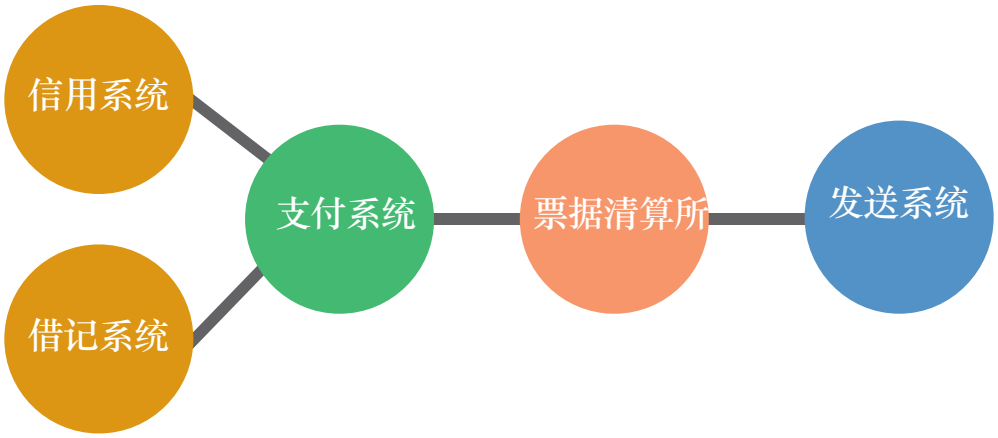
每个分布式账本技术网络都明确定义了其共识的政策和规则。 尝试通过验证具有不当行为的节点进行参与会遭到拒绝。 但是，某些分布式账本技术允许一组管理员同意用一组新规则来创建另一个账本以为它用，然后在新账本之间转移资产。 例如，某些分布式账本技术平台使用一组可由账本管理员修改的参数来定义账本的规则和策略。 然后，管理员可以通过向它们分配不同的参数设置来设置采用不同策略的账本。

分布式账本技术网络和非分布式账本技术系统之间的互操作性

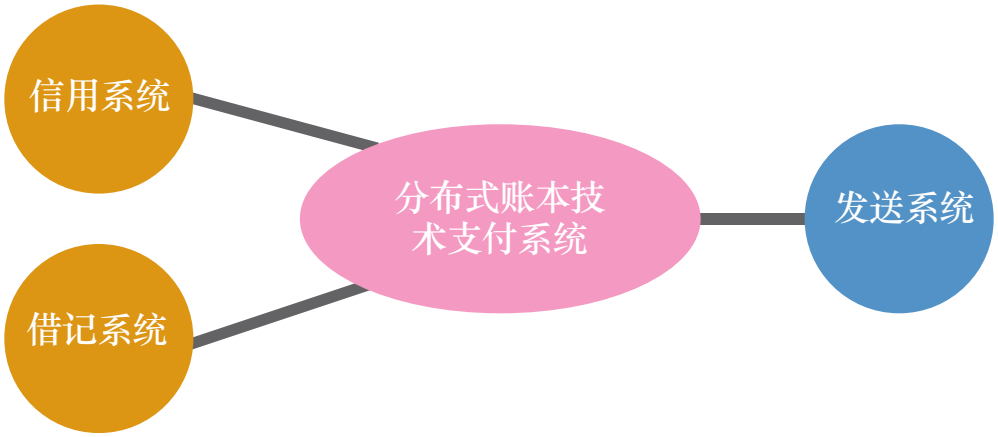
作为一种新兴技术，分布式账本技术已经开始在许多活动领域得到大量应用。然而，互操作性对于分布式账本技术能够与现有应用进行对接则非常重要。

例如，复杂的金融世界已经拥有一整套多元化的金融交易系统，它们共同执行许多不同类型的金融交易。虽然其中一些可能逐渐迁移到分布式账本技术之下，但该过程只能是渐进的。这意味着遗留的金融系统和新兴的分布式账本技术系统将在同一时间中共同工作，这就需要在遗留系统和分布式账本技术系统之间建立一种接口机制。

这种互操作性必须覆盖控制路径和数据路径。可能需要不同的接口方法以适应不同的非分布式账本技术系统。例如，在从非分布式账本技术系统接收数据时，接口设计需要决定数据是由验证节点拉取到分布式账本技术平台上还是由非分布式账本技术系统推送到分布式账本技术平台上。



a) 简化遗赠支付系统区块图



b) DLT 与遗赠支付混合系统区块简化图

数据拉取与数据推送之间的选择

数据推送/拉取之间的选择需要基于一组应用标准，包括数据新颖度和数据响应速度。

当验证节点想要从非分布式账本技术系统主动发起数据转移时，拉取数据模式较为适合。这允许它在需要数据时获得数据访问，并且避免接收其不需要的数据。例如，假设所需数据是由非分布式账本技术系统提供的不断变化的资产价格。验证节点不需要知道当日资产价格的所有变化，而只需知道智能合约指定的特定时刻的价格。在这种情况下，数据拉取模型更合适。然而，由于数据首先通过非分布式账本技术系统和分布式账本技术网络之间的屏障，在获取数据之前将经历某些延迟。当分布式账本技术系统中的多个验证节点获取相同的外部数据时必须小心。需要确保即使存在网络延迟，数据也是一致的。

当验证节点希望某一特定数据可获得时能够得知这一数据，推送数据模式是合适的，这一数据会被存储在本地以便在必要时进行后续获得。如果数据在其生成后不发生改变，也是合适的。在这种情况下，验证器随时可以对本地存储数据进行访问，并且不需要担心数据是否过时。更复杂的接口可以使用拉取和推送数据模型的混合。

很显然，解决互操作性问题越来越重要，因为更多的分布式账本技术平台开发需要与传统平台接口。

6. 分布式账本技术平台

比特币标志着基于区块链的分布式账本技术的引入。从那时起，分布式账本技术平台的设计出现了快速演变。具有各种特征和特性的平台不断出现，开发者可以在其上开发不同的应用。

分布式账本技术平台可以分为两大类：有中心的分布式账本技术平台和无中心的分布式账本技术平台。在无中心的平台中，账本通过公共网络中的节点之间的协作动作来维护，并且任何人都可访问。在允许平台中，参与仅限于成员节点之间：账本由授权节点维护，并且只能由注册成员访问。有中心的平台使快速交易验证能够实现，增强了隐私性，并且，操作可以消耗更少的能量。

不同类别的分布式账本技术平台也各不相同，具有独特功能。例如，一些平台用于特定类型的应用，而另一些平台用于一般用途。本章简要介绍一些最流行的分布式账本技术平台。读者可参考本文档“平台和应用程序部署的注意事项”中的技术说明（III），以获取更多信息。

6.1 比特币

比特币是中本聪在2008年作为数字资产和支付系统引入的无中心的分布式账本技术。它支持称为比特币的本地加密货币。

根据中本聪的论文“比特币：点对点电子现金系统”，比特币具有以下特征：

1. 双方能够直接交易，而无需受信任的第三方
2. 交易是不可逆的
3. 双花是不可能的

任何人都可以加入比特币操作。每个用户创建具有在网络中能够标识它的唯一地址的“钱包”。地址带有一对用于签名和验证交易的加密密钥。通过这些地址发送和接收交易。

每个参与比特币的参与者保留所有交易的完整历史。尽管比特币账本中的交易没有加密，但用户的伪匿名不会被发现，因为只有用户的钱包地址是公开的。

用户发送的交易由挖掘节点验证。挖掘节点不断地将经过验证的交易收集到新的区块中，这需要解决数学上的难题。成功解决这个问题的第一个挖掘节点获胜，并获得奖励。然后将新区块添加到区块链并传播到网络。

6.2 以太坊

以太坊于2015年7月推出，是一个无中心的分布式账本技术平台，用于去中心化的应用7。与其他无中心的区块链平台一样，以太坊区块链由公共网络中的所有连接节点维护。交易验证和区块创建由验证节点（也称为挖掘器）执行。新创建的区块然后传播到网络。

以太坊为希望在以太坊虚拟机（EVM）上编辑区块链应用程序的任何人提供一个灵活的平台.8 EVM可以被认为是一个包含了许多不同的被称为"帐户"对象去中心化的机器，这些账户能够执行代码。帐户有两种类型：外部拥有帐户（EOAs）和合同帐户。 EOA通过私钥验证外部访问，合同帐户由其内部代码管理。智能合约是由用户添加到交易的计算机代码，并发送到账本进行部署。智能合约的执行可以由附加的用户发送的交易触发。将交易发送到EVM中的帐户需要支付少量费用，称为"气体"。该费用是对矿工的奖励，以补偿他们在执行交易验证和区块创建时在硬件和电力方面消耗的成本。

奖励以以太坊本地加密货币"以太币"支付。它可以交易或用作加密货币交易所的支付媒介，例如Coinbase钱包系统。 Ether的开发作为一种工具以促进对等智能合约的操作。

6.3 超级账本

超级账本（Hyperledger）是一个有中心的区块链平台9。它是开源的，代表了企业和行业为了推进商业交易的方式齐心协力的努力。

超级账本没有本地加密货币。参与仅限于会员。商业交易以通过不同的计算机语言编写的智能合约进行编码。交易是加密的，只有有权限的参与方才能查看。超级账本提供了成员资格管理服务和交易密码管理服务。验证节点验证事务交易并执行提交到账本的智能合同。与无中心的分布式账本技术平台不同，超级账本中的验证节点的努力不会获得奖励。

超级账本通过其算法插件接口支持多个共识算法。验证节点默认的实用拜占庭容错（PBFT）应用算法来实现区块链状态的一致性。

6.4 Corda

Corda是由R3联盟开发的许可分布式账本技术系统，R3是一家创新公司，主持了与一组全球金融机构的联盟合作10。它的出现受区块链概念的启发。然而，它在许多方面与许多其他的分布式账本技术平台不同。首先，其账本条目记录在不遵循区块链模式的结构中。其次，它主要用于管理、记录和执行企业之间的财务协议。 分布式账本技术操作和业务协议执行操作在安全管理、易于审计和符合法规的环境中执行。第三，个人账本数据的共享仅限于具有合法需要知道和查看协议中的数据的各方11。

其共识机制也是独特的。它不是从系统层面上实现共识，而是对个别交易实现共识。支持不同类型的共识。但是，交易仅能由指定的验证节点验证。

实际上，交易中的企业可以开发以智能合同形式起草业务协议的应用程序。 Corda是可以执行智能合约的平台。协议被验证并记录在账本中，然后在Corda的安全环境中由指定的验证节点执行。

只有注册会员才能参与Corda操作，以保护交易协议的保密性并确保其安全执行。 Corda没有本地加密货币。

6.5 瑞波币

Ripple是一个专门为金融交易开发的有中心的分布式账本技术，是对当前的直接银行到银行支付系统的改进。它使银行能够通过多个网络实时发送国际支付。分布式账本技术使Ripple能够立即支付款项，而传统结算可能需要几天才能完成。这是通过即时记录付款指令及其在分布式账本技术系统内的执行来完成的。

在分布式账本技术中执行付款指令降低了银行和运营商的成本，同时缩短了结算周期。另一个好处是交易的完全可追溯性，操作可也是可审计的。

共识是基于一种称为InterLedger协议（ILP）的协议，该协议基于实用的拜占庭容错算法。该协议运行在不同的银行账本系统之间和且不受国界限制13。

由于银行受到高度监管，Ripple旨在通过支持风险管理、遵守合规要求以及保护隐私权，与银行的基础设施和实践相匹配，并通过使用加密技术保持交易的保密性。

Ripple有一个称为XRP的本地数字资产。对于执行银行支付交易来说并不需要。然而，它的定位是为跨境支付创造具有竞争力的外汇市场。

7. 治理

分布式账本技术网络，无论是有中心的还是无中心的，都需要采取某种形式进行治理以确保其正常运行。治理结构可以作为由原始设计者建立的一组操作规则开始。然后，这些规则根深蒂固地存在于分布式账本技术软件的设计中并嵌入其操作协议中。规则旨在管理和控制分布式账本技术网络及其参与者的行为和操作。

7.1 参与者制定规则过程

形成一套初始规则

无中心的分布式账本技术网络通常由一组开发者设定，这些开发者通常也是设置策略和规则的开发者。由于这样的网络大多数时间是开源的，因此随后的规则更新也对公众建议开放。如果被开发者组接受，则该建议被添加到用于分布式账本技术网络的现有规则中。

许可的分布式账本技术网络的形成可以涉及多个授权方。作为创始方，他们直接参与初始规则制定的过程，或者将此任务委托给其他人。比如说，R3Cev，一个由多个金融机构组成的联盟。14这些金融机构一起为各种金融服务定义了分布式和可复制账本的规则集。

规则更新

在大多数情况下，无中心的分布式账本技术网络没有中心化权威机构。它运行在内置于分布式账本技术软件中的固定的一组书面规则上。优点是，没有人变动规则，或强迫他人变动规则。这与无中心的分布式账本技术网络的去信任性很好的匹配。制定新规则或更改现有规则需要对软件进行修改。随着分布式账本技术得到了更多的认可度并被更广泛地使用，一般人群不可避免地需要新的功能和对错误进行修复。这需要适当的变更控制程序，允许添加新规则或修改现有规则。该过程从用户和开发人员对更改达成共识开始。然后开发人员修改软件。最后，由矿工决定是否转移到新编集的/更新的软件，即修改过的分布式账本技术网络。

这个过程的长度取决于多个因素。其中，争议的紧迫性和级别是主要的。对于紧急的错误修复，获得用户和开发人员之间的共识通常不难。由于矿工要保证分布式账本技术网络的安全、健全和平稳运行，他们通常更愿意采用新软件来解决出现的任何问题。

在一些情况下，可以提出不会从整个群组（包括矿工和用户）获得支持的新规则。在这种情况下，将出现支持者和反对者，问题的解决可能变得困难。

在这样的情况下，原始分布式账本技术网络可以分成两个不同的网络。一个组可能最终采用新软件，而另一组则坚持使用原始软件。然而，预测这样的结果是不现实的，用户和矿工/验证节点之间的民主过程将决定态势将如何演变。例如，如果矿工/验证节点的偏好由他们可能收到的交易费用的大小驱动，他们将选择提供最大交易量的网络。当然，也取决于用户喜欢使用哪个网络。

在许可的分布式账本技术网络中，规则制定过程类似于无中心的分布式账本技术网络—它也需要软件修改。然而，由于验证节点的循环仅限于注册的或授权的成员，所以该过程通常更容易和更直接。一个原因是，验证者一般来说具有共同的利益和共同的目标。在分歧的情况下，更容易让具有共同利益的利益相关者共同解决这个问题。如果分布式账本技术网络在中心化信任方的管理下，则该问题可能变得更加简单。

在允许分布式账本技术网络的情况下，设立缔约方建立监督和监测功能作为治理结构的一部分，是个很好的建议。这有助于确保坚持遵守规则和冲突解决程序，并有助于在分布式账本技术网络上正确管理访问控制。

7.2 明确角色和责任

不同群体的人会参与到分布式账本技术网络中。它们可以根据其功能分组如下：

开发人员

开发人员负责实施DLT协议，包括设置策略和制定规则。开发人员的组成影响此过程的操作方式。在开源DLT网络中，开发人员可以分为两组：核心开发人员和非核心开发人员。任何人都可以将其软件添加至网络。他们的添加由核心开发团队进行检查，以验证其质量和检查其功能，再由核心组决定是否接受它。

一般公众或非开发人员也可以在DLT软件开发中发挥作用。虽然他们不开发软件，但他们对新功能或变化的意见对核心开发人员在需要更改软件时的决定有影响。

在被接受之前，对软件的任何修改都应该遵守变更控制过程和质量检查。此外，开发人员应确保更改的软件经过充分测试并被用户接受。重要的是，必须保持和更新正确的系统文档，以确保正在进行的系统维护和系统支持能够顺利进行。

验证节点

验证节点的角色是验证交易并将其添加到DLT总帐。另外，无中心的DLT验证节点执行计算密集的区块挖掘操作，以创建有资格被添加到DLT账本的经验证的交易的区块。验证节点参与它们之间达成共识的过程，以保持账本的可复制副本之间的一致性。验证节点对于DLT网络的操作至关重要，因为它们提交大量资源以提供DLT平台所需的性能和安全性。虽然许可的DLT网络中的各方愿意进行这种投资，但是在无中心的DLT网络（也称为矿工）中的验证节点寻求获取奖励，作为对该进程付出了大量计算资源的回报。

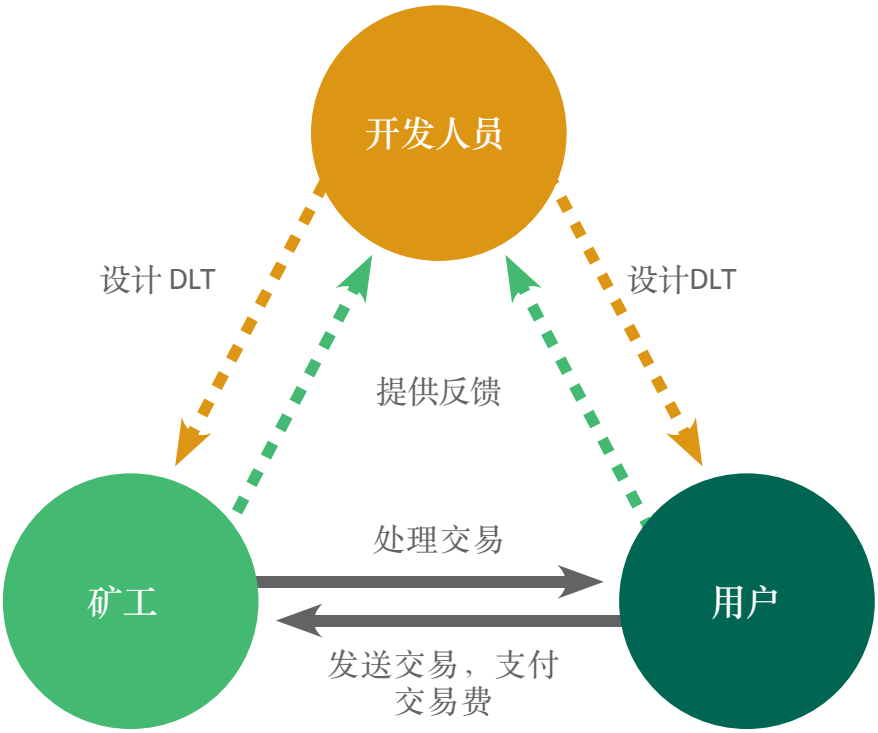
用户

DLT网络的用户在网络中进行交易，例如，通过进行支付，与其他当事方签订合同，转移资产所有权以及执行其他活动。虽然没有被严格地视为他们的角色，用户实际上发挥了重要的功能作用：他们保持DLT网络活跃和可操作。向DLT平台发送交易的用户，使验证节点的交易处理能够进行。

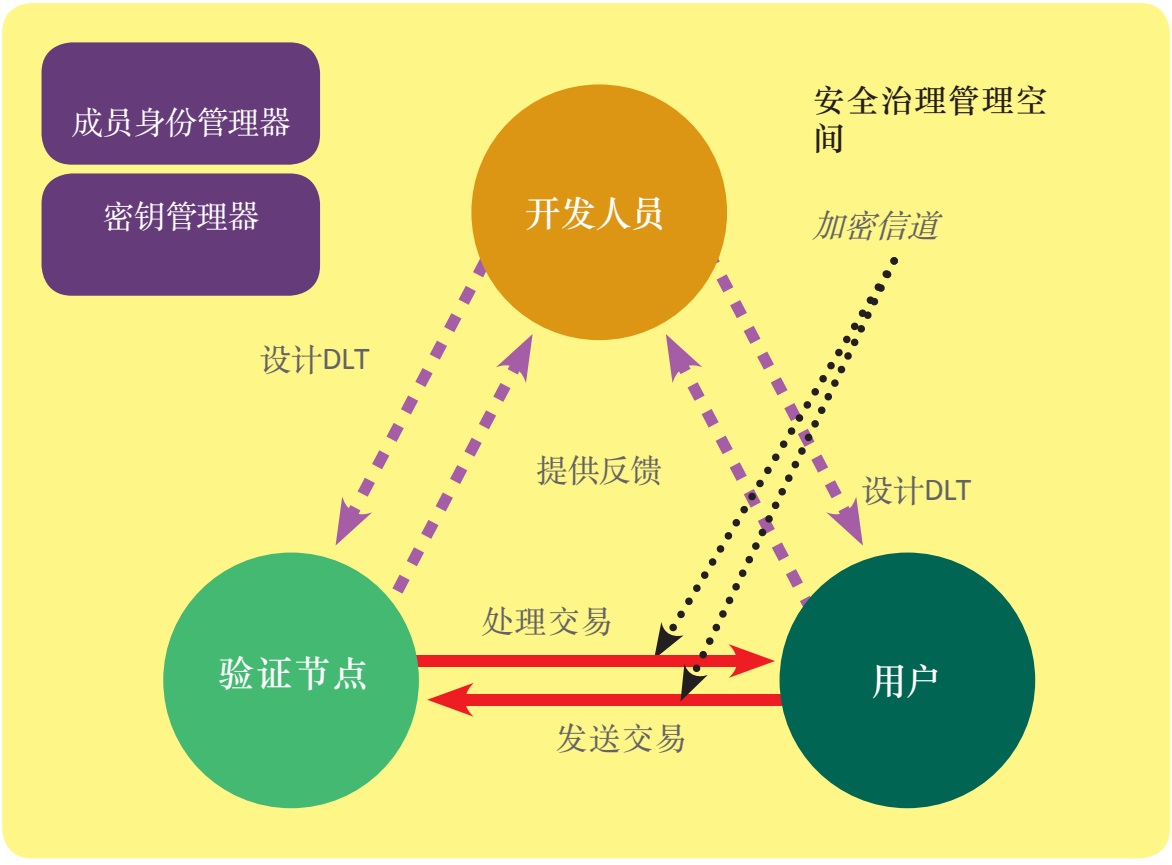
在无中心的DLT网络中，用户的角色通常是向矿工奖励交易费用。没有交易费用，无中心的DLT网络中的矿工可能几乎没有动力将其计算资源贡献出来以实现操作。

成员管理器和密钥管理器

许可的DLT网络具有另外两个角色：控制对网络的访问以及控制每个交易的内容。这两个角色需要成员资格管理器和密码密钥管理器。成员资格管理器控制成员加入网络。如果网络中的交易被加密，则密码管理器与成员资格管理器一起确定哪些用户将被授予对以简单形式进行的交易的访问权。



无中心的DLT网络中治理结构和参与者作用



有中心的DLT网络中常见的管理结构及作用

7.3 冲突解决

当新交易被发送到DLT　P2P网络时，该决议由遍布P2P网络的验证节点检查和处理。此验证是基于在DLT平台中设置的规则完成的。一旦验证过程完成，交易就由验证节点合并到一个区块中，然后将该块链接到账本。

验证完全符合DLT规则。还设置规则以解决由于DLT网络的性质而可能出现的冲突。然而，也可能出现需要外部干预的其他类型的冲突。

交易验证

验证过程包括检查不正确的事务语法和不符合DLT网络状态的情况。交易语法检查通常包括，检查以确保强制信息的存在、数字签名的真实性以及任何账本账户地址的有效性。违反DLT网络状态的示例是，账本指示之前已经花费的资产由于交易而出现双花。

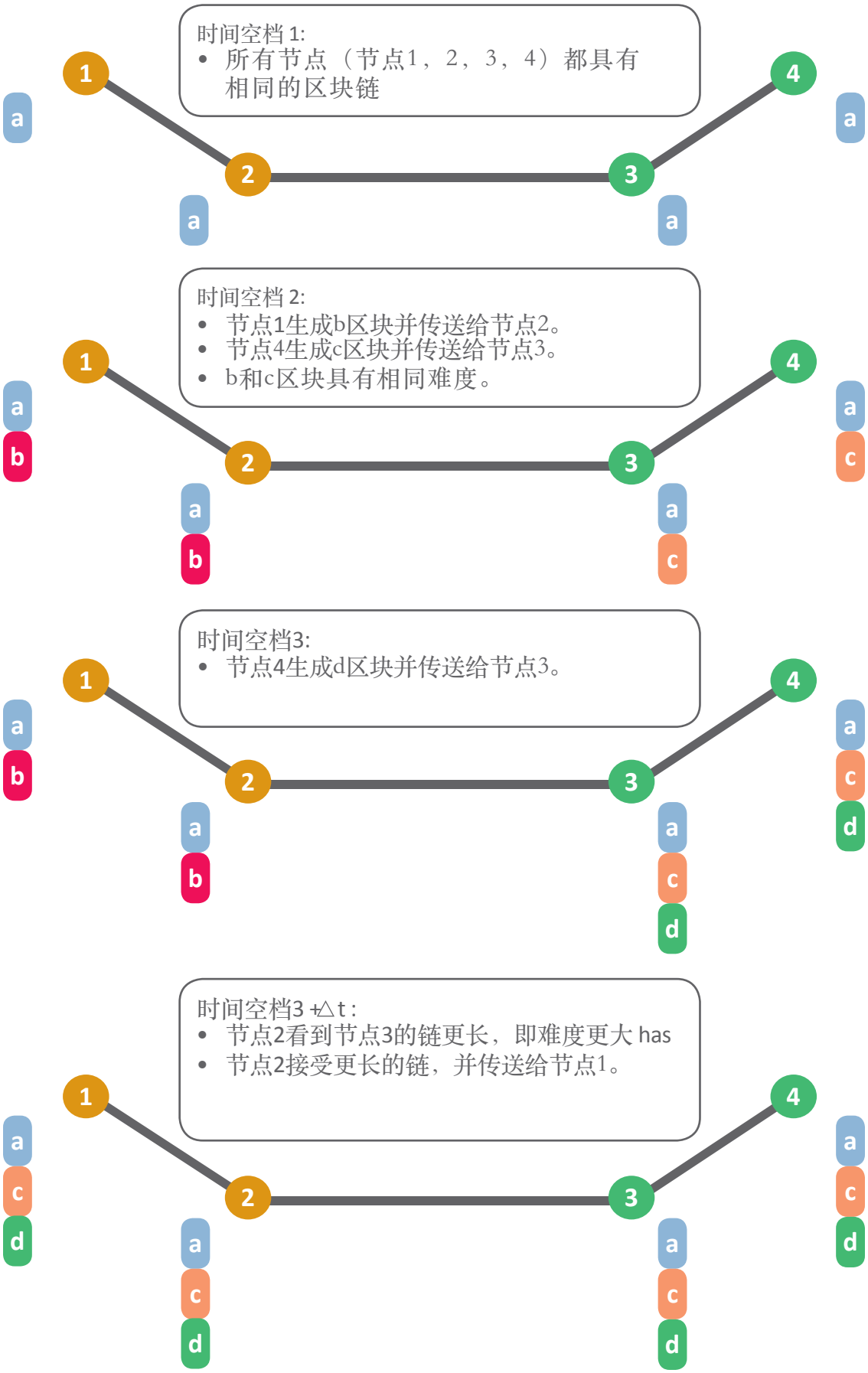
例如，在加密货币支付交易中，进行检查以确认存在必须记录在账本中的支付资金的来源。接下来，进行检查以发现资金是否仍然可用，或已经用完。如果发型任何不符合之处，则拒绝该交易。

账本自动解决的冲突

由于DLT系统是由在物理上分离的多个验证节点管理的可复制数据库之一，所以可能出现这样的情况：验证节点看到系统的当前状态的快照。例如，验证节点可以看到其他验证节点看不到的事务。 DLT协议应该有明确的规则来解决这种冲突。

如果两个矿工持有出现矛盾的帐本的副本，他们应用共识算法来解决差异。在使用挖掘工作证明的无中心的DLT平台上，在两个相矛盾但有效的帐本之间进行选择的规则总是涉及到选择较高难度的账本。由于帐本实际上是一个交易区块链，如果交易区块链比其他帐本中的链长，则该帐本有更高的难度。如果两个链具有相同的难度，则依然可以解决，但是它需要更长的时间。这是因为，虽然矿工的一个营地持有一个账本的副本，另一个矿工持有另外一个账本，任何首先成功开采下一个区块的矿工将拥有最新和最长的链。这个新扩展的链将传播到两个阵营。由于这个新扩展的链现在是更高的难度，所以它将被所有人接受。

其证明见下图。


时间空档 1:
• 所有节点（节点1，2，3，4）都具有相同的区块链
时间空档 2:
• 节点1生成b区块并传送给节点2。
• 节点4生成c区块并传送给节点3。
• b和c区块具有相同难度。
时间空档3:
• 节点4生成d区块并传送给节点3。
时间空档3 +△t :
• 节点2看到节点3的链更长，即难度更大 has
• 节点2接受更长的链，并传送给节点1。

在这方面，确保不诚实的矿工不拥有大多数采矿权见显得非常重要了。否则，这些矿工将始终成为第一个成功解决工作量证明问题的人，并生成最长交易块的链。这是众所周知的51％风险的例子。

有中心的网络，如Ripple15和Hyperledger，采用不同的共识算法来解决帐本冲突。一般来说，这些算法解决了拜占庭容错问题。拜占庭容错问题指的是一组拜占庭将军处于不同位置的情况，需要找到一种沟通共同计划的方式：攻击或撤退。他们必须达成共同协议。该算法是为了制定在这种情况下达成共识的方法。

需要外部干预的冲突

DLT可以处理部分是由于分布式分类帐的固有性质引发的事件，诸如由于网络延迟导致的短时不一致性等。然而，即使DLT网络被正确地实现并且网络处于正常状态，仍然可能发生只有通过人为干预才能进一步解决的其它事件。

说一个比特币的例子。当前的比特币区块大小限制是1兆字节。统计表明区块通常可容纳2,000项交易，每项交易约500字节。随着比特币用户群的扩大，交易的数量也在增加。一些人认为需要解除区块大小限制以便适应越来越多的交易。然而，不是所有的利益相关者都认为更大的区块符合他们的利益。例如，驻扎在具有较低网络带宽位置的矿工可能认为自己处于不利地位，因为它们的网络不能应付交易流量的增加。16如果一项决议被达成，其采用也必须通过人为干预来执行：即通过更改比特币软件并在比特币节点中安装新软件。

在大多数DLT网络中，没有中央管理机构来负责、管理及控制网络的操作。这样的操作模型与常规系统基础设施和操作模型有很大不同。所以，理所当然需要一种新的治理框架和治理结构，应该建立一个持续监督和管理DLT网络的机制。在本研究项目的下一阶段将进行进一步研究，以确定对监管可能产生的影响，以及为监管机构制定一套控制原则。这将有助于在金融服务中更广泛地采用DLT。

8. 风险管理与法律遵从

一些推荐的DLT平台将在公共网络上部署和操作，金融交易可以通过网络传输并由这些DLT平台处理。此类平台可能涉及的操作风险则不能被忽视，包括操作风险、网络攻击和洗钱问题。本章旨在确立一个大致的风险列表，并思考其对DLT开发的影响。与上一章中提出的治理问题一样，在本研究项目的下一阶段也将进行风险管理问题的进一步研究，以制定一套关于下文提出的风险的控制原则。

8.1 操作风险

恶意验证节点

DLT共识算法应具有从DLT网络检测、识别和排除恶意验证节点的能力。例如，病毒感染的验证节点可能会将包含错误或未授权决议的区块添加到DLT网络中。任何尝试改变交易历史或添加虚拟交易的攻击都应能够被其他验证节点迅速检测和识别，并且通过共识算法妥善处理处理。

网络故障和网络攻击

DLT网络上的DLT节点可能遭受网络故障问题和恶意攻击。虽然网络堵塞等网络故障可能只导致通信延迟，但是诸如分布式拒绝服务攻击（DDoS）或目标网络攻击等恶意攻击可能会导致一些验证节点失效。在正常情况下，DLT网络拓扑是为了能够承受任何临时网络中断问题。多个验证节点的存在还使得网络能够应对针对所选验证节点的DDoS攻击。然而，还有其他形式的DDoS能够攻击所有的验证节点，他们通过目标特定的验证功能和利用网络传播攻击。由于DDoS攻击的类型不同，可能需要新的预防和补救性反击措施来防止这种攻击。

8.2 身份盗窃风险

DLT网络内的人通过提供数字签名来证明他或她的身份。由于需要私钥来创建用于识别自身的数字签名并且证明对资产享有所有权，所以资产的所有者必须妥善保护私钥以保护资产。如果私钥被盗，行为人可以作为所有者改变资产的所有权。

所有者有责任采取措施确保私钥安全，确保私钥安全。同时应对私钥进行加密，确保只能由授权用户访问。通常情况下，“冷存储”为在线密钥存储提供更好的保护。在冷存储中，私钥是离线存储的。冷存储的示例是Trezor设备，这是存储私钥的安全令牌。当需要对数字化交易进行签名时，将数字化交易转发到安全令牌进行签名。

虽然正常用户私钥的丢失可能与DLT平台的完整性、安全性和健全性没有任何直接关系，但是私钥的丢失可能导致未经授权的资产所有权被转移，这又可能在很大程度上破坏DLT平台用户的信心。

8.3 行为风险

洗钱

非法获得的法定货币可以通过货币兑换转换成加密货币，然后通过DLT平台进行一系列交易以隐藏货币来源。因此，如果没有足够的洗钱控制，如DLT平台上的用户身份验证（KYC）规则和交易监控控制，DLT平台可能会被用于洗钱活动和资产的匿名转移。

销售非法药物和违禁品

犯罪分子可以使用DLT平台作为非法毒品和走私物品的支付平台，或作为非法资产交换平台。同样，客户身份验证措施和交易监控控制对于DLT平台至关重要，特别是在这些平台允许公共用户参与的时候。

接收勒索付款

近年来，勒索软件计算机病毒的出现，攻击了许多个人和商业计算机。黑客有时要求受害者将赎金存入黑客伪匿名的DLT“钱包”。

应当谨慎对对未来DLT可能出现的不当行为进行预判。建立有效的风险管理系统和程序，确保应用程序中的任何故障不会扩散到DLT平台而破坏该平台的稳定性，或影响公众对平台完整性的信心。同样，也要确保对DLT平台的任何攻击不能危及到用户的DLT资产的安全。

采取充分的预防措施和检测措施，最大限度地减少滥用的机会和操作中断的风险。随着密码学的不断进步，这将是一个持续的挑战，因为用户可以使用密码隐藏他们的交易细节。

DLT平台运营商应实施用于记录和分析那些可以检测可疑活动的系统活动的工具，还应该开发更先进的报告和交易响应系统。此外，应制定强有力的交易连续性管理框架和相关安排，以应对对DLT平台的任何严重破坏。

8.4 法律遵从

所有监管当局的主要目标都是保护金融和银行稳定，保护消费者合法权益。这就是为什么金融和银行部门要受到严格监管的原因。金融和银行服务对DLT越来越感兴趣并越来越多地采用DLT，这显然对监管当局造成越来越大的压力。

一般来说，DLT的合规性仍然是尚未开发或尚未得到深入调查的领域。到目前为止，监管当局几乎没有颁发布监管指导或控制原则的方法。此外，某些推荐的DLT平台的分散性和跨境特点让监管变得更复杂。这也引出了以下三个问题：应该管制哪些活动、如何管理活动以及应该由谁来管理。虽然如果监管机构只是采用传统的监管方法（鉴于其技术中立态度），似乎最为直接了当，但本白皮书列出的一些与DLT相关的关键风险和法律问题，如果采用这种方法，是否能够得到妥善处理，尚不可知。

法律遵从当然是一个需要关注的领域，但需要在实施正式监管之前进一步研究。本白皮书旨在对DLT进行深入调查和审查，并列出其使用中可能涉及的风险和问题。希望为本研究项目的下一阶段奠定良好基础，包括为监管机构确定良好的监管指导和控制原则。

9. 安全和隐私

9.1 安全

无中心的 DLT网络

如前面章节所述，在无中心的DLT网络中，提出的假设是没有矿工是可信的。为了保护无中心的DLT网络的完整性，设计了挖掘机制以确保没有矿工能够通过创建虚构区块和交易来欺骗或利用其他矿工。这些机制包括已在第四章中详细讨论挖掘工作证明。

类似地，假设无中心的DLT网络中没有用户是可信的。为了防止对其记录在无中心的DLT网络中的资产进行双花，矿工要核对资产交易历史并比较他们的DLT账本的副本。这种比较，通常被称为共识过程，是使矿工能够检测无中心的DLT网络中不诚实用户双花问题的机制之一。

虽然资产所有权在无中心的DLT网络中可见，因为所有人都看到交易，所以在资产可以交易和转让所有权之前，需要资产所有者的数字签名。这不仅适用于资产交易，而且适用于无中心的DLT网络内进行的所有交易。

为了防止任何故障或盗用，或DLT账本副本的消失，可复制副本由物理上独立的矿工保存和维护，确保了（除非所有可复制的副本均被破坏或修改）无中心的DLT网络及其记录的交易保持的完整性。

有中心的的DLT网络

与无中心的DLT网络一样，无中心的DLT网络也使用密码学来进行记录保护，但是方式更广泛。

只有经授权方才允许加入有中心的DLT网络。这降低了不诚实的验证节点错误地处理许可DLT网络的操作，以及盗用网络内的交易记录的风险。诚实节点仅在通过安全认证之后才能访问有中心的DLT网络，例如通过验证注册成员的数字签名。

通过使所有验证节点运行共识过程，确保它们对将被添加到DLT账本的交易，从而提供进一步的保护。这确保了DLT账本的可复制副本的健康、完整和一致，同时也有助于隔离由于技术故障或其他问题而发生异常的验证节点。

9.2 隐私

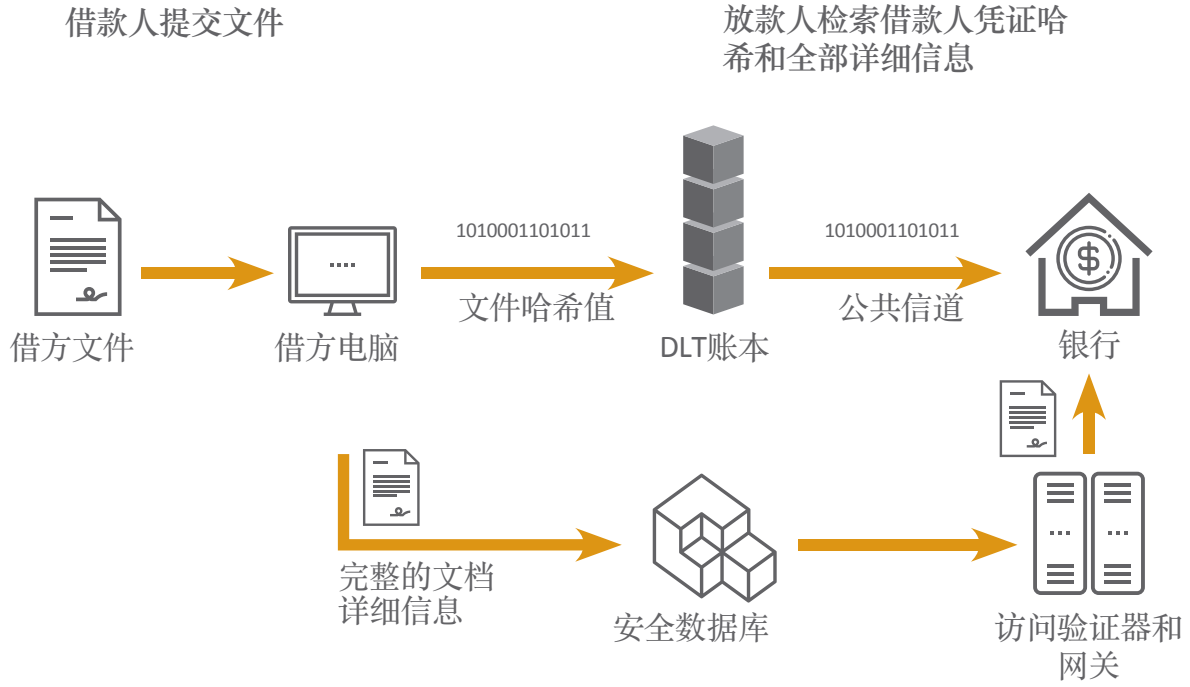
无中心的DLT网络

用户身份是伪匿名的，因为只有有限量的个人数据和身份信息存储在无中心的DLT网络中。尽管无中心的DLT网络中的交易通常是未加密的，但它们只能被追溯到DLT钱包地址，DLT钱包地址是与钱包相关联的数字串，但是它不揭示钱包的私有（秘密）密钥，并且不暴露太多钱包所有者信息。这有助于保护隐私和隐藏所有者的身份。

用户可以通过利用不同的DLT钱包地址来进行个别交易以进一步保护他们的交易历史的隐私。[17] 这使得其他方非常难以追踪所有者的身份，或者识别存储在无中心的DLT网络的交易和资产的所有者身份。

有中心的DLT网络

在有中心的DLT网络中的交易被加密以防止未授权方读取它们。验证节点和用户之间的网络通信也被加密以使数据难以理解，即使这些加密数据在许可的DLT网络的数据传输期间被截取。通过在受限位置存储机密数据，DLT分类帐仅存储该数据的哈希，数据隐私可以进一步得到保护。



图示反映了 DLT 账本中文件哈希值的存储

虽然只有注册会员可以参与有中心的DLT网络，但会员的身份不一定在交易中显示。为了保持成员的活动历史是私有的，当进行新的交易时，DLT平台可以向每个成员分配交易证书。这意味着成员发起的不同交易可能使用不同的交易凭证。因此，其他成员只能将交易与特定凭据相关联，并且无法从中推断出该成员的身份。一些有中心的DLT网络利用这种方法通过以交易证书的形式出具匿名成员凭证来保护成员的隐私和他们的活动历史。18只有授权的审计员被授予访问会员信息的权限，并且能够将交易证书与会员的身份联系起来。

9.3 挑战

无中心的DLT网络

潜在不诚实多数攻击

无中心的DLT网络的完整性依赖于这样一种假设：拥有大多数采矿能力的大多数矿工在采矿和维护网络方面是诚实的。如果大多数矿工有机会聚合在一起，或者几个不诚实的矿工拥有大部分的挖矿能力，这些矿工将能够损害无中心的DLT网络的完整性。

DDoS（分布式拒绝服务）攻击

虽然矿工的多样性和P2P网络的高互通性使得无中心的DLT网络难以被DDoS成功地攻击，使得该攻击完全被击败，但是这种攻击仍然可能会降低DLT网络的性能，或暂时分裂DLT网络。这暴露了对高网络性能和弹性操作的需要，从而防范此类攻击。

窃取电子钱包密钥和其他风险

记录在无中心的DLT网络中的资产如果其私钥被盗就会有风险。可以使用多个数字签名的方式实现加强安全控制的第三方托管服务，例如在签署交易时不仅要求所有者的数字签名，而且还要求来自DLT网络中的可信任第三方的数字签名。

然而，私钥仍存在被盗取的威胁。已经出现了私钥被从加密货币交换中和在加密钱包中被偷走的情况，盗窃有可能让一些加密货币交换的操作崩溃，导致严重的资金损失和随之而来的用户信心的暴跌。

盗窃事件

根据一些新闻报道，比特币和以太坊都出现了被盗事件。然而，没有证据表明这些事件是由DLT的技术设计或DLT协议问题引起的。相反，有些盗窃事件是黑客发动的，他们利用了用户开发的保护私有密钥安全的软件中的错误或漏洞。

据新闻报道，Bitfinex是一个遭受过黑客攻击的交易公司。黑客设法破坏了公司的系统，并从其用户帐户取走了119,756个比特币。该公司本来实施了一个系统，用户可以在这个系统上在线存储比特币，方便用户更容易访问他们的比特币帐户。该公司与BitGo合作实施多签名保护方案，以防止在未授权的情况下访问用户帐户。尽管采取了所有这些保护措施，犯罪者仍设法通过系统找到一种破解方式，并从用户的账户窃取了比特币。[19]

隐私挑战

此外，当面临既需要保护用户隐私又需要协助执法机构执法时，对于无中心的DLT网络，始终存在挑战以及在某些情况下的困境。政府当局希望能够查证非法加密货币活动，如洗钱、逃税、贩毒和赎金。另一方面，用户可能担心他们的加密货币活动的细节被暴露从而他们的个人数据和生活方式的细节可能会暴露给未授权方。为了不同的正当目的，用户保护隐私的需要与当局的知情权及监督权之间的冲突所带来的挑战不可小视。

有中心的 DLT网络

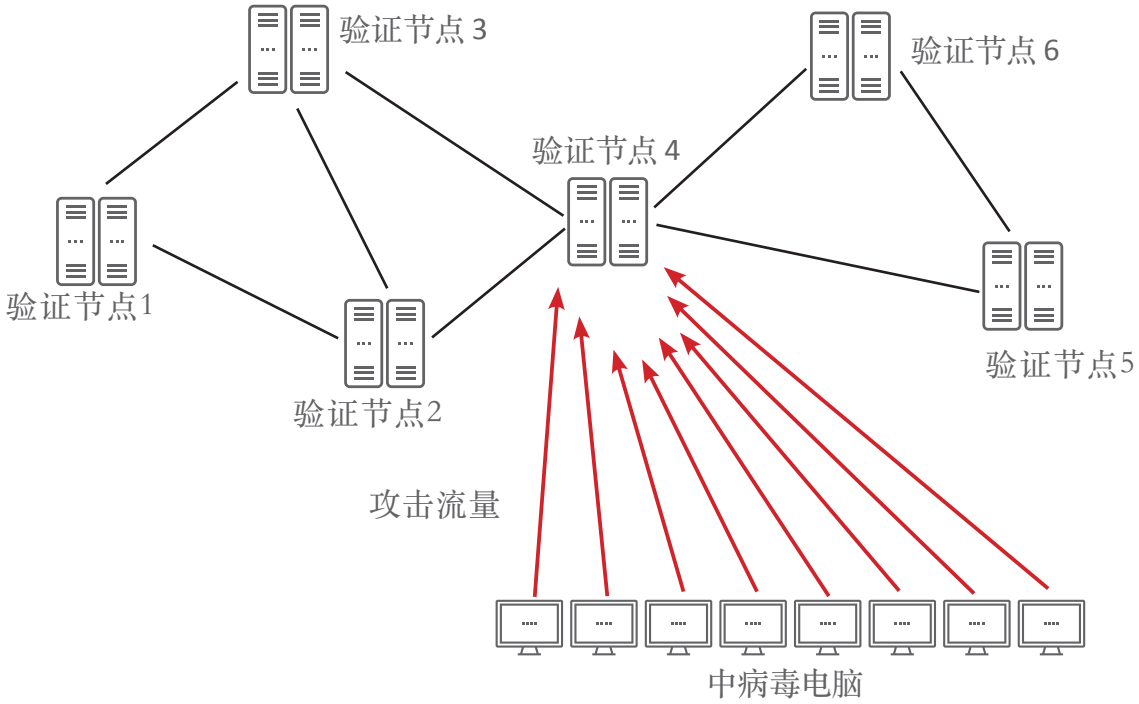
安全漏洞

攻击可以有多种形式，如DDoS，植入病毒或恶意软件等，因此应该采取预防和检测措施。DDoS攻击的风险可以通过监视和检测工具，也可以通过网络设备来减轻，这种网络设备应可以检测和转移DDoS包到被隔离位置以进行分析和适当处理。应对系统和通信软件进行检查和审计，以消除任何可能的DDOS攻击漏洞。系统必须由防病毒软件保护，并且系统上运行的所有软件在安装前都应经过严格的更改控制管理过程。

有效管理

有中心的DLT网络需要实施有效的管理，允许管理员监视、配置和控制DLT网络，以保持其完整性和顺畅运行。在病毒攻击、网络中断或其他情况下，网络管理团队应有权修补损坏之处并使网络恢复正常运行。更重要的是，应建立一个强大的业务连续计划（BCP），以解决可能出现的任何意外情况。20,21此外，使所有验证节点在BCP上和在DLT网络上采取的任何应急措施达成合意是一个巨大的挑战，所以在编制一个有中心的DLT网络时，应该在这个问题方面投入足够的时间和资源。

(a)网络碎片问题



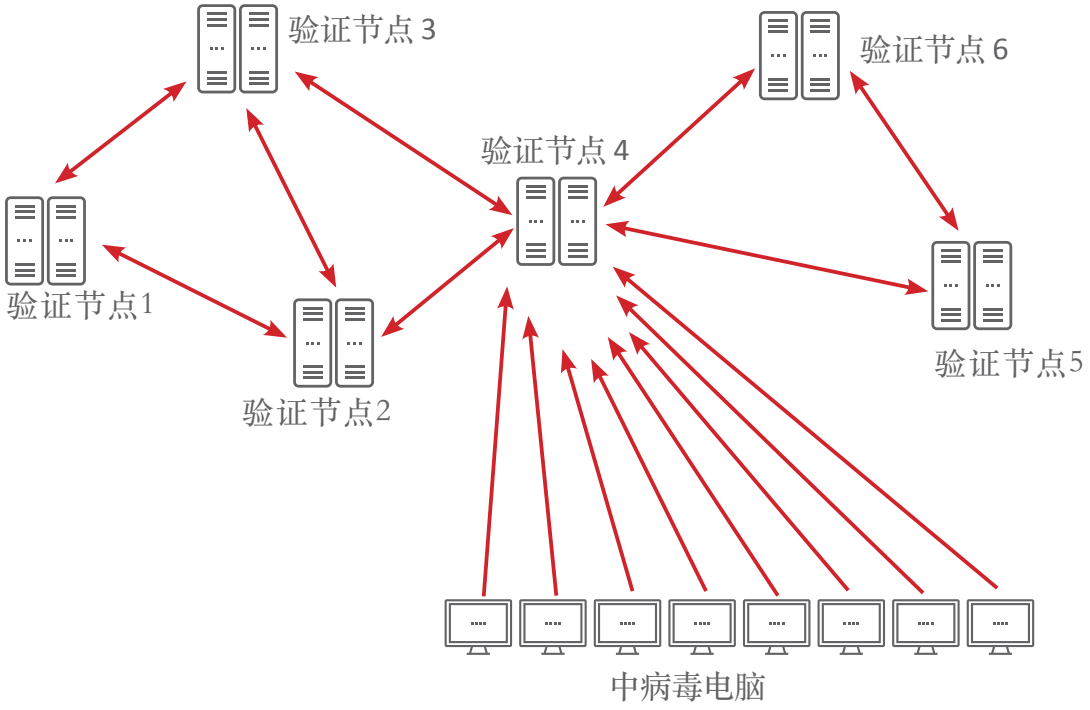
图示: DDoS攻击一个单独验证节点

在上图所示的简化DLT网络系统中，P2P网络在节点4处是脆弱的。如果节点4受到攻击并且不再能够在其左侧和右侧的节点之间转发分组，则P2P网络将被分裂成两个网络碎片：

碎片 1: 包括节点 1, 2 和 3
碎片 2: 包括节点 5和6

虽然这是DLT网络的简化图示，但是其证明了对于有中心的DLT网络来说，在验证节点之间提供足够的连接和冗余度以避免出现网络碎片是多么重要。

(b) 网络性能问题



图示： DDoS攻击了所有的验证节点

在上图中，DDoS攻击将合法交易发送到验证节点4。交易没有关闭节点4，而是利用包含使所有验证节点投入大量资源的指令来处理和验证它们。由于交易是合法的，所以验证节点4将处理交易并将它们传递到要进行的相同进程的其他验证节点。这可能导致整个网络的性能遭受损坏，因为该过程需要大量计算资源而导致发生严重损坏。

上面的两个例子显示了DDoS对DLT网络操作的可能影响。因此，必须采取充分的预防、监测和补救措施，以防止针对DLT网络的此类攻击。

隐私挑战

许可的DLT网络中的敏感交易数据通常需要进行保密，并且对这种数据的访问应该仅限于授权方。强大的数据加密和足够的访问控制对于保护有中心的DLT网络至关重要。有中心的DLT网络应该仔细设计，在系统设计阶段嵌入安全和数据保护要求，并在实施之前进行彻底审查。

节点可以用于存储账本或数据库的目的。随着DLT账本中处理数据的新应用的开发，需要新的加密技术对数据进行安全保护。例如，对存储在DLT账本中的记录执行新型大数据分析可能会需要新的加密技术。为了确保DLT网络的安全性和高效率，期望能够以加密的形式对这样的记录进行大数据分析。此外，计算能力（例如量子计算）的进步有可能使当前加密技术被破坏。随着时间的推移，总是需要新的加密技术来进行更高级别的保护。

解决平衡数据隐私和数据透明度的挑战，以便官方可以执行某些行动，有中心的DLT网络显然是一个更好的选择。有中心的DLT网络能够以满足数据隐私要求同时符合执法机构和监管机构的要求的方式进行设计。例如，由于有中心的DLT的成员是信任的和已知的各方，被接受的操作规则可以规定它们需要遵守当地法律和法规要求。

10. 法律思考

显然，DLT已经引入了一种与业务合作伙伴和客户相关的全新业务往来方式。由于其独特的分布式特性和在帐本中记录交易的方式，它不仅具有减少错误和欺诈机会的潜力，还提供了更高水平的数据访问和灵活度。虽然DLT有可能为仍处于探索或采纳它的早期阶段的许多组织带来好处，但其非常规和独特的特征可能会产生与其最终可采纳性相关的一些法律挑战。

由于关于与DLT有关的法律考虑的讨论需要律师和其他法律专家的意见和深入研究，本白皮书并不试图就DLT问题提供任何详细的法律指导。相反，它旨在指出一些潜在法律问题可能产生的影响。后续需要对DLT进行更详细的法律研究，并应由法律专家进行。应科院计划邀请有兴趣的法律专家在下一阶段参与这项研究，以便为银行业提供更高层次的法律指引。

与数据隐私有关的法律影响

DLT网络可能涉及个人数据的存储，例如在第三章中描述的Alice和Bob之间的虚构财产交易中，个人资料被记录在DLT账本中。对个人数据的处理产生了与法律和合规要求相关的主要问题。如果在香港进行个人资料处理，《个人资料私隐条例》(PD(P)O)的规定便会具有现实意义。

《个人资料私隐条例》规定了若干主要原则，以确保由机构收集的个人资料得以妥善储存，直到无继续保存必要的，并且只能用于收集个人资料时的目的。数据的使用者还需要采取实际步骤保护这些个人数据免遭未经授权的使用，并使他们的个人数据原则和做法为公众所知。

鉴于DLT的去中心化和分布式性质，所涉及的客户应充分意识到他们的个人数据在DLT平台的所有参与方之间共享。在各参与方之间应建立适当的治理结构，通过商定的机制对客户进行应有的通知。 DLT平台还可能需要制定一组商定的规则和策略，由所有参与方遵循并且告知客户。

即使允许在DLT平台的参与方之间共享个人数据，也应进行适当的管理，以明确和认可数据被搜集的目的，并确保此数据仅用于明确规定的目的。在参与方希望将收集的个人数据用于新目的时，应当获得客户同意，并且该同意应在DLT平台中规定的账本记录访问策略详细指示。

DLT的一个主要优点是它的不可篡改性，意味着数据不能被改变或删除。然而，这可能违反了应该明确个人数据的数据保留期限，并且当不再使用或当客户请求时应该删除或清除数据的要求。

解决这个问题的一个潜在方法是使用密钥为每个数据添加一个额外的加密层。不是清除整个记录，而是仅删除特定数据的密钥。然而，对密钥对管理应进行更深刻的考虑，并应进行测试以验证实用性。此外，在开始实施任何政策之前，需要在其中一些领域提供适当的法律咨询。

上面讨论的与隐私问题相关的问题让无中心的DLT网络。变得更加复杂。由于没有管理网络的中央管理员或机构，没有人对任何风险承担责任。这当然是DLT的独特之处，但也带来了一些重大的挑战。

诉讼和法律纠纷

无论DLT网络是有中心的还是无中心的，有缺陷的代码或程序错误都可能对特定参与者造成损害或财产损失。DLT的去中心化使得难以在法庭上寻求追索权。DLT网络不是以单个公司的形式，而是以一组参与者的形式连接在一起以执行某些商业活动。可能没有任何中心化管理员或权威机构对有缺陷的操作设计或参与者的不当行为负责。在最坏的情况下，网络可能像一个绅士俱乐部，成员自担风险加入该俱乐部，不受任何公司法保护。

为了说明这一点，我们采用第三章中的例子，Alice在无中心的DLT网络中将她的房产卖给Bob。假设，由于代码缺陷，Alice在几天后才收到付款，即使房产权已在约定日期成功转移给Bob。因此，Alice不能解决未偿还的按揭贷款问题，并因为未按时还贷受到了银行高额的罚款。由于没有DLT平台的中心化管理员，特别是在无中心的DLT网络中，Alice很难找到任何负责任的个人对其财产损失负责。如果买方和卖方都用的是匿名身份，情况会变得更加复杂。

代码中的规则和条件

传统上，每个法律或具有法律约束力的交易都涉及到某些法律文件。对于Alice和Bob之间的房产交易，这些法律文件包括交易的正式买卖协议、更改房产所有权的所有权契约以及B银行和Bob之间的抵押协议。

在未来的DLT世界中，所有合同都可以用计算机代码（即智能合约）起草。这就产生了法律界和律师事务所是否意识到并为此做好准备的问题。如果发生争议，律师也必须审查计算机代码。纸质合同明确地以易于阅读的方式编写，因此所有相关各方都可以理解。然而，用代码编写的契约涉及在代码逻辑中定义的条款和条件，这对于未经训练的法律人来说是难以理解的。因此，提供DLT合同起草和分析工具将是确保合同的准确性和完整性以及这些合同中的条款和条件的有效步骤。

遵守法律法规

与上面讨论的许多问题一样，缺乏中心管理员（特别是对于无中心的DLT网络）使得难以对系统操作进行某些基本维护活动，以及实现对各种法律和规章的一般遵守（例如与数据隐私、反洗钱要求等有关的）。此外，跨境交易或与跨境DLT平台的连接提出了与法律的适用性和可执行性相关的更多的重大问题。

在第十章的工作概念证明中论证的按揭贷款申请概念证明，已经明确了一些真正的法律问题，这可能需要改变现有法律，以使DLT模型运用于在现实世界。迄今为止，大量的努力和资源已用于证明该技术的可行性，但对对法律影响的重视不够。

国际动向

应科院从金管局得知，中央银行和监管机构充分认识到法律问题对进一步发展DLT的重要性。于是，成立了一些关于数字创新的数字创新工作组来审查这些问题。以下列出来金管局明确和在讨论的主要法律问题。其中有些与本章所述的应科院的意见相类似。

适用法

- DLT安排的适用法律是什么？这项法律如何可以执行，特别是在去中心化、无限制或跨国的发展中？
- DLT安排的规则、程序和过程的法律基础是什么？
- 参与者之间（包括在跨境活动中）在何种程度上可以被视为建立了有效、有约束力和可执行的合同安排？
- 如果资产以数字形式在DLT账本上构成，那么数字形式的资产的法律依据是什么？

权利和义务

- 参与者和DLT安排的权利和义务是什么？这些权利和义务如何实施？所有参与者是否知道并理解权利和义务？
- 在什么条件下可以对参与者的权利和义务提出质疑？改变DLT安排中的权利和义务的机制是什么？

系统责任和义务

- 如果安排出现问题，谁应负责？如果没有中心管理者负责，责任问题的争议机制是什么？

可执行性

- DLT安排如何设定和执行其规则、程序和合同，包括谁参与制定和执行？该DLT安排如何在相关的情况下跨越国界执行其规则、程序和合同？
- DLT安排的工具如何有效地及时执行其规则、程序和合同？这些工具会在法庭上被支持吗？如果这些工具在法庭上无效，那么实际的法律、财务和业务影响是什么？

这些法律问题不那么一目了然，不能仓促解决，需要更多的研究工作、需要法律专家的研究和投入，来确保这些法律问题得到有效的处理。在本章结尾，是Carla L. Reyes教授的论文《分布式账本技术将推动法律创新》。在论文中，教授分享了她关于DLT在美国不仅适用现行法律，而且也对政府对法律的制定、实施和执行提出的设想带来了基本思路。

分布式账本技术将推动法律创新（作者：Carla L. Reyes教授）

革新。这个词是企业家，监管者和学者对头脑中出现频率最高的词。虽然这本身并不罕见，但这次新一轮的创新讨论可能比以前的谈判更关注技术对法律的破坏性影响。各个国家和国际组织已经表示越来越意识到需要监管创新，以与近期的技术驱动的行业创新相匹配。在美国，各联邦和州法律制定和监管机构专门考虑技术创新对其任务、方法和目标的影响。行业似乎很高兴看到他们对监管思维的转变产生影响。例如，当美国财政部货币审计长办公室发表题为《支持联邦银行系统中付责任的创新：OCC视角》的文件，并呼吁公众进行回应时，至少有六十二（62）个个人和单位提出评论。

虽然其他颠覆性技术是监管机构目前全力应付的创新之一，但分布式账本技术正是许多监管讨论的中心问题。与关于创新的讨论一样，分布式账本行业似乎一般都希望监管机构和政府在制定法律政策和确定执行优先级时参与其中。例如，美国卫生和人类服务部收到了对其关于使用分布式账本技术改进卫生信息技术和卫生相关研究的建议的七十（70）份答复。这种对合作的开放应该加强，特别是在监管重点转移到去中心化账本技术（例如，比特币作为支付机制）的支付应用时，并探讨该技术在其他领域的应用。

到目前为止，对比特币和作为支付机制的其他加密货币的监管极大地受到了传统支付监管的影响，没有灵活的监管创新来适应去中心化账本技术的独特性质。结果是，至少在美国是，一个面临对分布式账本上交易的数字资产的分类相互矛盾的行业。美国财政部将加密货币视为"代替货币的价值"，因此应受到依据所讨论的商业活动的货币传输管制的制约。同时，美国国税局将加密货币归类为财产。商品期货交易委员会对若干行业参与者采取了执法行动，表明根据对其的使用，加密货币可能受商品法规的制约。州法官和州立法机构还就分布式账本上交易的数字资产的分类表达了不同的观点。这些同样的联邦和州管理机构正在将注意力转移到分布式账本技术的其他使用案例，包括与产地、证券交易、不动产记录、隐私记录和提高政府运行效率有关的法律问题的有效记录。在此过程中，与行业的公开对话可为技术及其使用案例以及其他实质性法律领域制定更新的监管方法开方便之门。这样，分布式账本技术不仅颠覆了现行法律的适用，而且颠覆了政府设想的法律的制定、实施和执行的方式的基本要素。这种法律的颠覆只会使受管理者受益，无论是产业界还是消费者，如果受管理者和受控制者共同面临法律创新的挑战。

11. 概念证明工作

根据金管局的委托，应科院与香港多家银行及相关业界人士合作，包括汇丰银行、渣打银行、中国银行（香港）、恒生银行及东亚银行等，探讨了将DLT应用于银行业的几个子用例的可行性。在与参与银行商讨后，金管局和应科院决定在三个范畴进行概念验证工作：按揭贷款申请、贸易融资和数字身份管理。对于每一个领域，已经建立了一个行业工作组，讨论概念验证计划，制定概念证明工作的范围和设计，以及在金管局- 应科院创新中心进行概念验证工作。

截至2016年10月底，用于进行房屋估价以用于抵押贷款申请的DLT原型已在建成的最后阶段，并正在进行测试。关于其他两个领域（贸易融资和数字身份管理），概念证明工作相对更复杂，需要进一步研究，从而最终确定最佳的运作模式。尽管每个子用例的进展情况各不相同，但我们想借此机会分享其在提出的DLT解决方案，经验教训，实施经验以及利益和建议方面的现状。由于所有三个子用例都需要更多时间来完成概念验证工作，因此在本研究项目的下一阶段（明年某个时候）将提供对每个子用例的进一步更新。

在附录中，我们还给出了由R3联盟和IBM提供的一些共享，这些共享解决DLT在按揭证券（MBS）和贸易融资的应用，为DLT的应用提供了不同的视角。

11.1 概念证明 - 抵押贷款申请

简介

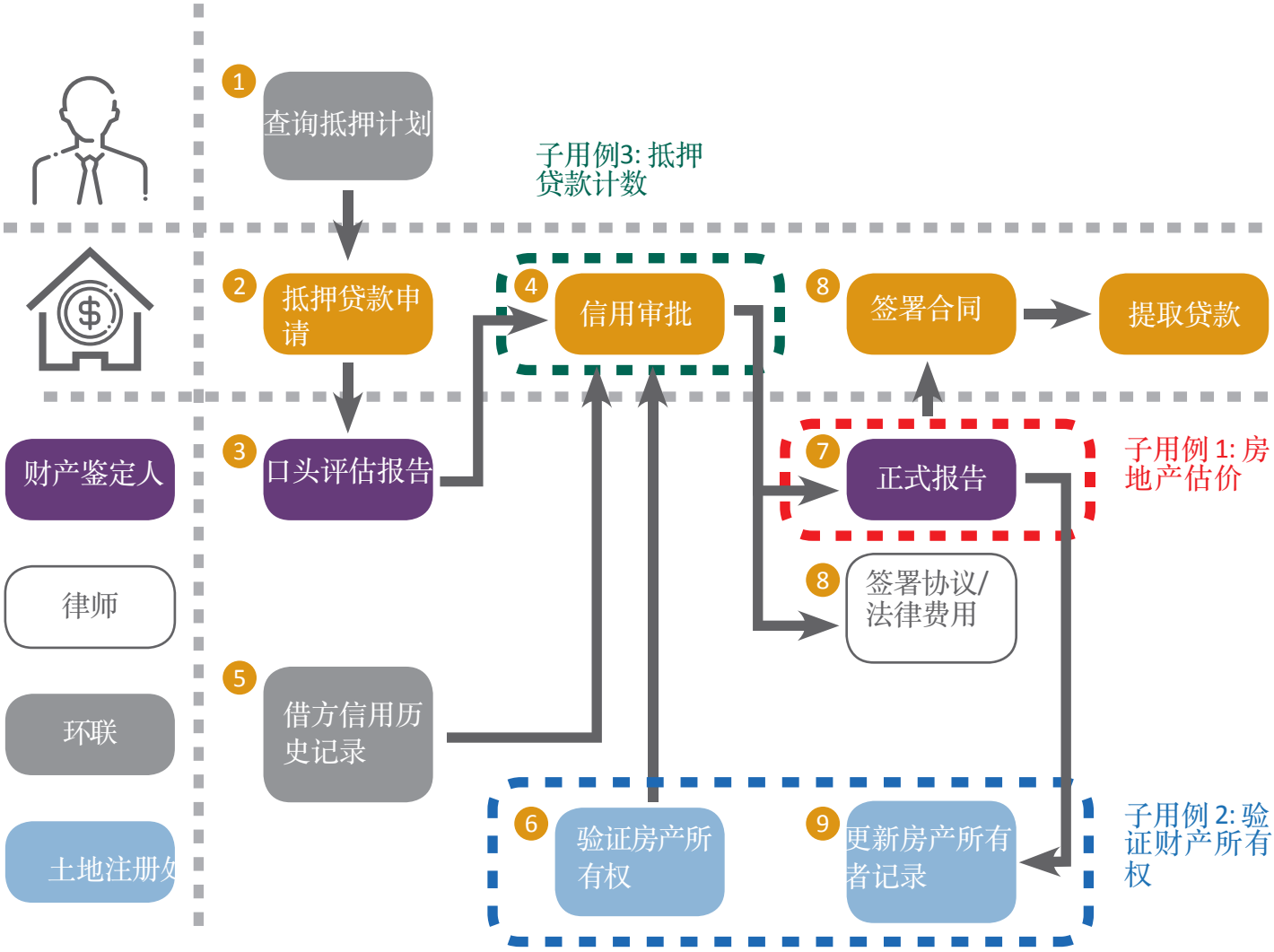
抵押是一种基本的融资工具，为抵押申请人（抵押人）提供资本资源，以购买房产，或通过使用房产作为抵押获得融资。由于抵押贷款通常涉及大额贷款和长期贷款，银行有义务在处理抵押贷款申请时进行充分的尽职调查。

目前的按揭贷款申请程序耗时、费力，需要大量人力且以纸张为基础。它还需要多方参与，例如抵押申请人（财产所有者）、银行（融资来源）、鉴定人（进行房地产估价）、律师（处理所有法律材料）、信用局（即环联），以及土地注册处（保存最新的产权所有权清单）。

与其他五家参与银行一道，金管局和应科院已成立一个按揭贷款工作小组，研究将DLT应用到贷款申请程序的可行性。

抵押贷款申请程序

目前从银行获得抵押贷款的过程如下：



流程描述:

1. 当买方和卖方达成协议处理房产并签署买卖协议（S&P协议）时，买方可以向多家银行提出抵押计划。

2. 银行派遣鉴定人进行对房地产进行初步估价，用于提供预计按揭贷款额。当买方决定向哪家银行提交按揭贷款申请时，申请流程开始。 首先，买方向银行提供所需的信息，包括银行对账单、收入证明，买卖协议和其他现有贷款信息，以及同意从环联公司（一家消费信用报告公司）获取信用报告 。

3. 银行要求鉴定人提供口头估价结果（通过电子邮件或传真），以确定抵押贷款金额。

4. 银行根据买方和其他外部方提交的信息开始信用审批流程。

5. 银行会要求环联的信用报告以查询买方的历史信用记录，包括任何不良信用信息和买方的抵押贷款计数（即买方未偿还抵押贷款和个人贷款的数量）。银行使用这些信息做出信用决策。

6. 银行在土地注册处进行财产土地检查，以核实买卖协议中所述的所有权。

7. 在签订任何法律文件之前，银行要求鉴定人邮寄最终的估价报告，并使用此报告对含有信用审批结果的财产状况进行验证。

8. 银行向买方提出要约，并通知律师安排签订按揭贷款协议和抵押契据。

9. 在所有法律文件定稿之后，律师将已签署的按揭契据发送给银行，以便银行可以安排提款，并向土地注册处发出通知以便更新地契。

按揭贷款申请程序的三个主要范畴

如上一章所示，完整的抵押贷款申请流程涉及多个耗时的步骤，并且还需要一些子流程来衔接多个不同的参与方。工作组确定了DLT的应用可能会改善当前的抵押业务工作流程的三个领域，分别是是财产估价、财产所有权验证和抵押贷款计数。

为了简化研究，工作组做出了以下三个假设：

- 银行可以共享抵押贷款相关数据的DLT网络可能包含敏感的个人数据。有鉴于此，工作组认为DLT网络应以私人模式运作。只有授权方才允许接入DLT网络。

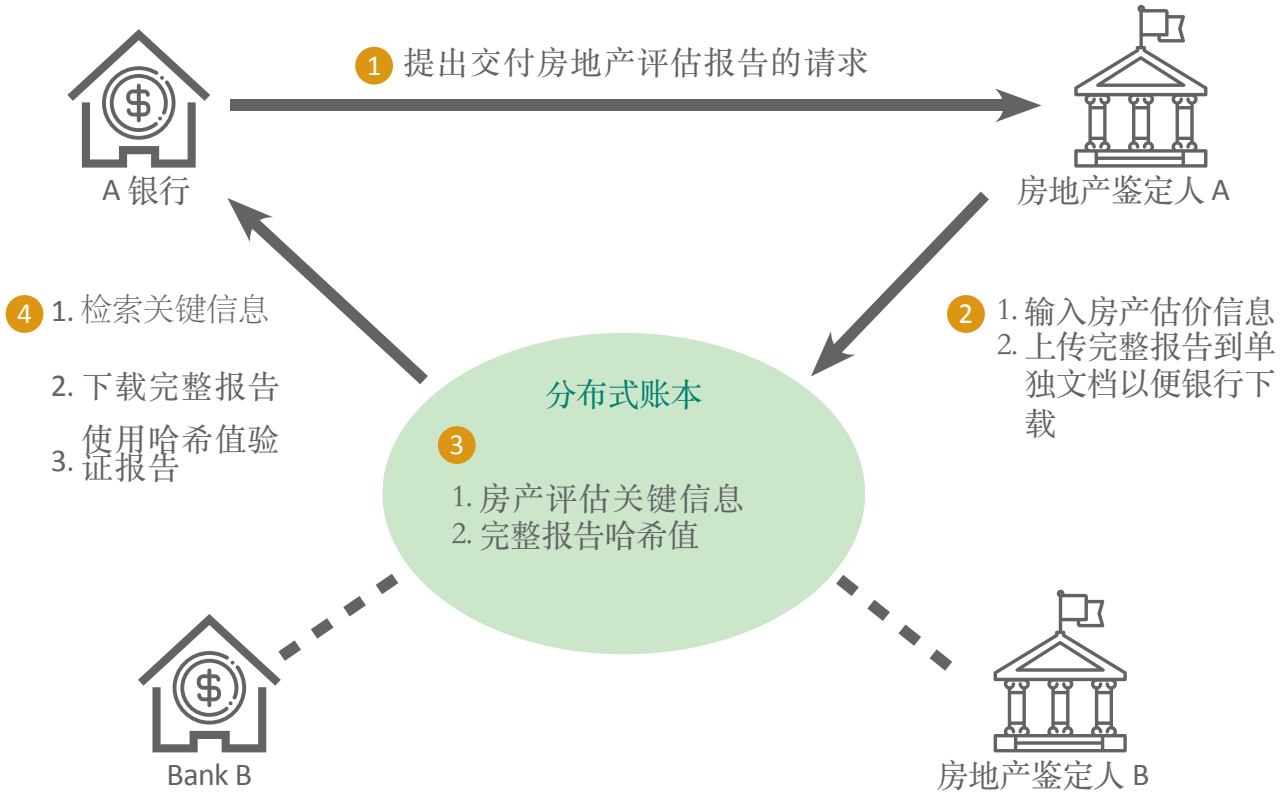
- 按揭贷款申请程序涉及多方，例如律师、信贷局和土地注册处。这些当事方的参与可能涉及建立商业安排，甚至修改法律框架（这将在本章后面讨论）。为了简化研究，我们假设银行是DLT网络的唯一参与者，除非另有规定。

- 由于按揭贷款申请的子用例2和3要求银行业提供一整套信息，以说明假设所有银行都参与DLT网络的好处。

11.1.1 子用例1：房地产估价

财产估价报告评估有关财产的市场价值。 当财产买家从银行获得按揭贷款时，银行要求鉴定人提供估价报告。 这是为了确保所批准的按揭贷款额是该财产的市值估价相匹配，并确保该银行能够收回未偿还的款项，在该按揭尚未偿付。 在目前的业务流程中，银行有义务获得并在两年内妥善保存财产估值报告。

为简化鉴定人取得评估报告的过程，应科院已开发了一套DLT原型从而实现人工操作和纸质程序数字化。DLT原型可将数字化评估报告的关键数据和哈希捕获到分布式账本中并将其存储，这提高了过程的效率和安全性。



DLT房地产估价流程

流程说明:

1. 对于按揭贷款申请，A银行通过电子邮件或电话向财产鉴定人 A 要求提供财产评估报告。

2. 财产鉴定人A准备评估结果和完整报告。 然后，鉴定人输入结果，并通过用户界面将报告上传到分布式账本。

3. 网络节点生成完整的报告哈希值，并将最重要的财产评估信息（包括财产地址、价格和区域等）存储在分布式分类帐上。

4. 银行A从网络检索评估信息，并使用哈希值来验证报告。

当前流程不足：

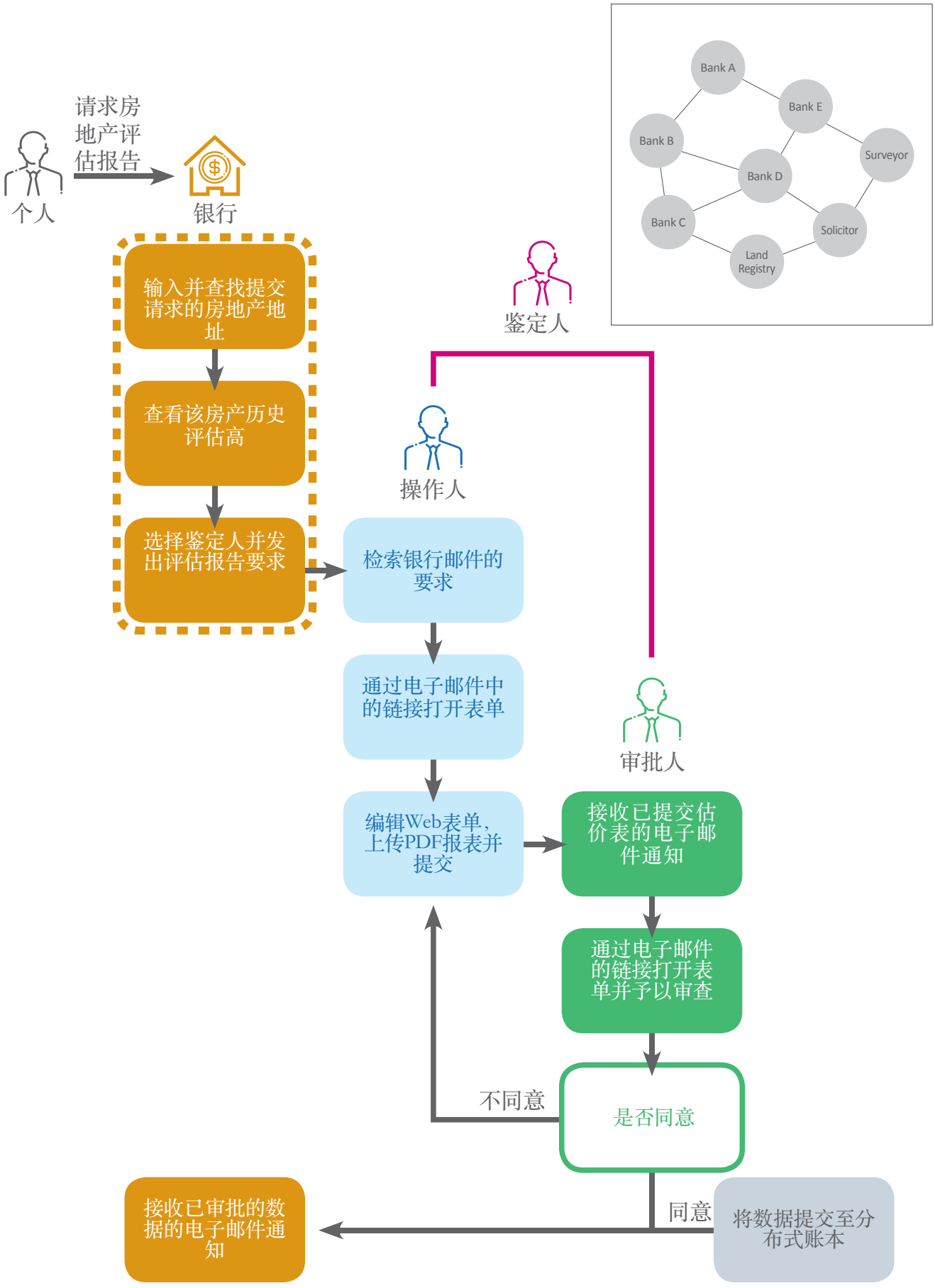
- 需要纸质房地产评估报告
- 没有对数字化评估报告的版本控制，并且很难验证报告的数字副本
-

DLT实现的改进：

- 估值报告可以数字化
- 规范整个行业的数据格式，确保过程完整性
- 提高抵押贷款申请的效率
- 改进了评估报告的安全保护。对报告未经授权的更改很困难
- 可以节省物理存储空间

概念验证的发展涉及构建用户界面，鉴定人能够从银行接收评估请求，并将重要数据从数字化估值报告提交到DLT网络。　　工作组中大多数银行达成合意的的关键属性是：市场价值、财产地址、财产参考号、占地面积、完成的月份和年份、估价日期、完整的报告哈希值，评估公司的名称，以及财产类型。

在鉴定人完成审批程序后，这些数据将提交至DLT网络并与其它参与银行共享。



提交房地产评估报告至DLT网络详细流程

（工作小组）对初次合作经验进行总结

根据工作组其中一名成员的实际经验，以下是采用DLT进行财产评估过程的主要好处：

- *通过消除纸张复印报告对传输和存储，降低了操作成本*
- *简化流程，提高客户满意度*
- *新技术促进操作风险最小化*
- *在金融业内建立标准化抵押贷款流程*
- *使用无纸化操作实现了"绿色财务"*

房地产评估涉及非敏感和可公开访问的信息，因此它作为子用例是测试此新技术的的理想选择。此外，由于财产评估只涉及两种类型的参与者，银行和鉴定人，有中心的DLT的特征可以被有效地测试，而不需要涉及太多的不同方。

从抵押贷款申请证明概念工作的第一阶段来看，参与方会受益于能够产生信任的分布式账本技术的发展。 与贷款业务中的现有的人工或半人工的纸质化的房产评估过程相比，还能够以更有效地并且以更低成本的方式共享信息。 下一阶段的目标是在其他领域的流程中开展工作，以便DLT可以更广泛地应用于抵押贷款业务。 以下四个方面的讨论是从各成员实施DLT的经验中得出的：

1. 充分利用新系统及其可能的拓展的应用

假设客户Cathy从 C银行申请新的抵押贷款。C银行向房地产鉴定人发送一份评估报告请求。同时，C银行向DLT网络发送另一请求，以检查Cathy申请抵押的房产是否已经进行了其他抵押，或Cathy是否仍还有任何其他未偿还的贷款。 与传统的耗时、纸质的，容易出错和容易滋生欺诈的流程相比，基于分布式账本技术的该流程更有效、更具可靠性，并且因此有助于创建可信任的商业模型。同时，它提高了在抵押申请过程中进行的信用风险分析的质量。由于Cathy向C银行申请了新的抵押贷款，因此该流程提供了有关Cathy的额外信用信息，其他银行在以后对Cathy执行额外信用风险评估时可以参考（如果需要）。

房产评估子用例也有望扩大银行、鉴定人、律师及土地注册处等各方对新平台的参与度，这会在本章下面部分所讨论的子使用案例中发挥重要作用。

2. 技术和操作注意事项

成本是开发创新技术（如DLT）时的主要考虑因素之一。在DLT网络中，每个参与者需要构建其自己的系统并使其与自己的其它现有基础设施和相关策略兼容，特别是在网络安全领域。此外，在客户端系统安装、通用用户和管理员操作程序以及某些系统故障时的企业应急计划中缺乏对设置、操作及维护的指引。虽然实施双节点设计可以减少故障的风险，但是需要部署系统恢复过程。然而，应科院已经创建了一个DLT操作监控仪表板，它提供了一个警报系统，可以帮助成员处理这些意外情况。为了更好地管理网络，DLT需要一个专门的团队来承担此操作监视角色，以及分配软件程序并监督DLT环境的未来技术发展。

3. DLT平台的检测和审查

为了确保DLT平台的稳定和性能，需要进行不断的检测节点的健全性、个体成员的"友好性"、成员之间的交互性、系统功能完整性（特别是与安全性和隐私有关的功能）以及维护系统的难易程度，特别是当它涉及跨越不同参与者的许多不同的系统和治理策略时。定性和定量结果（例如用户体验、系统延迟、系统故障恢复时间等）将提供一种更全面的方法来测量金融行业的技术成熟度。

4. DLT对社区和社会的益处

DLT平台通过确保其数据集的完整性、可靠性和透明度，以提供全面的数据视图，使得授权方能够分析不同级别的信息（例如根据地理位置、财产价值层，财产交换频率或季节性趋势和季节模式不同等进行不同的分析）。这种分析的结果可以为政府重要的政策决定提供宝贵信息。此外，当利用诸如　利率和租金数据等经济数据作为补充时，有关房地产交易和抵押贷款的信息可用于进一步研究房地产行业，并帮助政府进行相关政策。

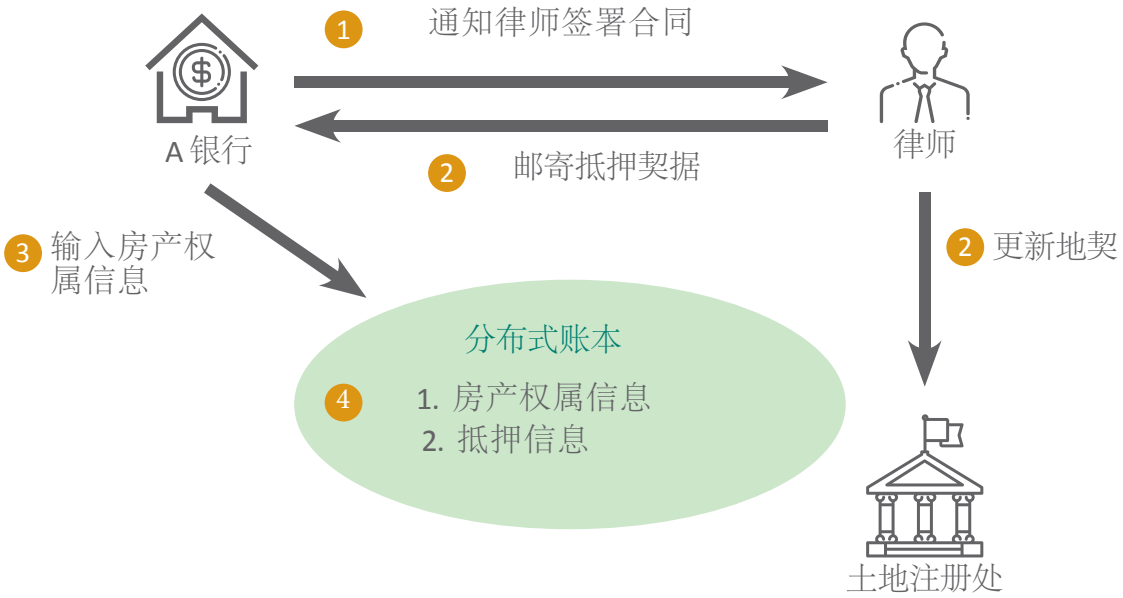
11.1.2 子用例2：验证财产权属

银行批准抵押贷款申请所需的信息包括财产所有权和抵押贷款计数信息。在目前的程序中，这些资料是根据《土地注册处条例》在土地注册处备存的，并且需要其它的程序和处理时间才能获取并进行更新。根据参与工作小组的银行提供的资料，从财产交易完成起至土地注册处所有权资料更新，最多可能需要40天。之所以需要这么长时间是由于需要手动处理多个过程，包括文档处理和传递，以及将信息输入到计算机系统中以及更新计算机系统。这么长的周期可以创造欺诈的机会。

根据工作小组提出的安排，银行将可以在分布式账本上存储按揭契据和所有权契据的数据，使参与的银行能够保持最新的财产所有权和抵押信息记录。加入DLT网络的银行越多，抵押记录的准确性和完整性就越好。

第1步: 将契约上传至DLT网络

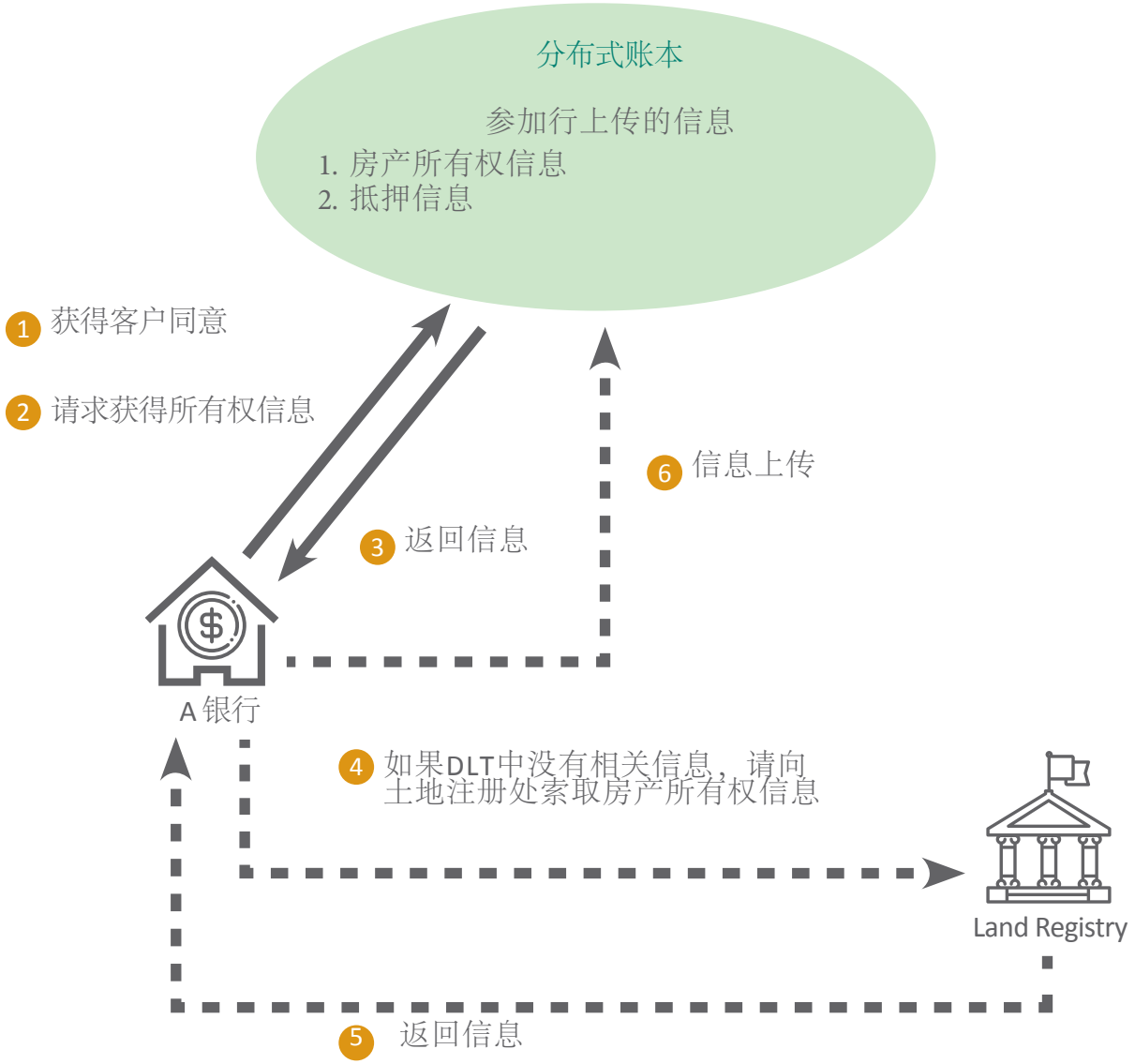
每完成一次抵押贷款申请，银行都会将新的抵押和权属信息上传至DLT网络：



流程介绍:

1. 信用申请一经审批通过，银行通知律师签署协议。
2. 贷款在所有权权转移日支付予律师，贷款及业权契据以邮递方式寄往银行，而所有权契据资料则送至土地注册处。
3. 银行将房产转移信息输入到分布式账本。
4. 分布式账本存储房产所有权信息和抵押贷款信息。 其他银行可以从DLT网络检索此房产所有权信息。

第2步: 如果DLT网络中未记录某一所有权信息，则从土地注册处检索该信息



DLT 所有权信息检索工作流程

流程说明:

1. A银行对房产所有权信息请求获得客户的同意
2. A银行要求提供房产所有权信息
3. A银行从DLT网络检索信息
4. 如果在DLT网络上找不到信息，A银行要求土地注册处提供房产所有权信息
5. A银行从土地注册处检索信息
6. A银行将更新的房产所有权信息上传到DLT网络

优点

由于需要一些时间来获得所有现有客户的一致同意（需要他们同意将他们现有的抵押贷款和所有权信息上传到DLT网络），因此最好在每次做出新申请时就进行上传。这意味着银行只需在短时间内就可以受益于这项安排。

缺点

银行可能需要几年时间才能将所有客户的抵押贷款和所有权信息更新到DLT网络，因为房产的所有权不会经常更改。一些房产的所有权可能30多年都不会改变。在所有财产都已上传到DLT网络之前，一些信息将不可避免地丢失，这可能对DLT网络的有效性产生影响。

当前流程不足：

- 由于需要复杂的人工流程，土地注册处可能需要很长时间才能更新所有权信息
- 更新信息的滞后性可能导致欺诈案件

应用DLT实现的改进：

- DLT能促进房产所有权信息在房产所有者、买方、银行和律师之间交换
- 提高获取最新房产所有权信息的效率
- 贷款和所有权信息可在DLT平台上获得，这有助于实施下一节讨论的子用例：抵押贷款计数

11.1.3 子用例 3: 抵押计数

在子用例2中，抵押贷款计数信息从第三方机构获得需要超过3个工作日，该机构作为代理机构向香港所有银行申请抵押贷款计数信息。抵押工作组建议抵押贷款契约信息可以通过DLT网络共享，从而提高业务流程的效率和准确度。

DLT抵押计数工作流程

流程说明:

1. D银行对房产所有权信息请求获得客户的同意
2. D银行要求获得借款人的抵押计数
3. DLT网络通过为获得此信息而开发的应用程序接口向成员银行发送请求
4. 成员银行通过该接口将信息发送至分布式账本
5. 借款人的抵押信息被存储在分布式账本中
6. 请求行（即，D银行）从分布式账本中检索包括借款人的按揭指标和相应的房产地址等。

当前流程不足：

- 从环联请求抵押贷款信息时周转时间长（长达3个工作日）

应用DLT实现的改进：

- 参家行能够在分布式账本上分享客户未偿还抵押贷款的数量
- 增强了整个流程等效率和准确度

抵押计数检查的增强

对某一房产享有的所有权显示了个人或组织管理该房产的权利，包括出售给他人，用该房产作为担保物以进行融资（抵押）等。如今，银行依赖土地注册处的记录，这就意味着任何所有权转让信息的更新都可能需要40天才能完成。

如果允许银行在分布式账本上直接更新注册信息，DLT的采用可以有效减少与地契更新相关的时间的滞后性。因此，抵押申请过程中，更新的记录可以几乎实时地提供给银行进行验证。

11.1.4 总结 - 益处和挑战

DLT的益处

DLT平台提供了一种不可变的、透明的和防篡改的方式，所有利益相关者可在所有可信方中即时发布数字化文档。贷款申请流程采用DLT可以促进纸质文件的数字化，并为抵押贷款申请留下完整的审计证明，从而大大节省了人力和存储空间，并降低人工操作出现失误的风险。交易记录可以在非常短的时间内添加在DLT网络中，着大大减少了文档收集和传送时间。它还提供了一个透明的、按时间顺序记录的日志，用于未来的调查和审计。此外，数字化文档可以减少对手动数据输入的需要，从而最大程度地减少人为失误的可能。而且，数据格式的标准化可以帮助行业利益相关者增强其记录管理程序，并简化其业务工作流程。

该子用例表明，DLT为纸质文档的标准化和数字化，以及为抵押业务流程的完整审计跟踪提供了一个很好的机会。在抵押业务流程中，有六种类型的文档可以被数字化并存储在DLT网络中。这些文档数字化相关的益处如下：

实施数字化的文档	益处
评估报告	• 规范银行与鉴定人传输评估报告及材料行为。
使用说明书和贷款提取书	• 规范银行与律师之间的数据流和数据输入。
抵押契据	• 共享已验证的的房产所有者、借款人及保证人的真实信息。 • 确保信息的连续性和透明性。 • 减少抵押欺诈和人工失误的风险。 • 提高对客户抵押贷款对评估效率。
权契证	• 可以节省物理归档和检索需要对人力。 • 提取贷款程序实现自动化。 • 验证房产所有权成为可能。
信用记录	• 促进对信用的评估。 • 减少信用风险。 • 降低中介成本。
其他地产检察文件（如，法院指令）	• 及时获得可能会影响估值结果和抵押贷款批准的重要信息。

挑战及下一步计划

在上述抵押贷款申请概念证明下讨论的所有三个子用例都有可能无可争议地给行业发展带来无尽利益。然而，许多问题对实际商业世界中成功采用该技术提出了挑战，特别是在子案例2和子案例3（财产所有权验证和抵押贷款计数）方面。下面我们讨论抵押工作组已确定的各种主要挑战，并提出一些可能的措施来解决这些挑战。

- **电子交易条例**

《电子交易条例》（第553章）附表1明确规定，《土地注册条例》（第128章）涉及到的任何契据、财产转让行为或其它书面文件或文书以及免责辩护，不适用本条例。这意味着这些文件必须是书面形式才具有法律约束力。

抵押工作组需要探讨修改《电子交易条例》（CAP 553）的可能性，以能够适用于数字方式存储和交易的契据、转让，文书、判决和未决诉讼。工作小组参考电子支票计划的判例，在该判例中，2014年，金管局与政府资讯科技总监办公室（“资讯科技总监办公室”）合作，修订“电子交易条例”（第553章），以让支票不属于附表1中所列事项，从那时起，电子支票就能够在银行和个人之间合法出具和转让。

- **《土地注册条例》和《产权注册条例》**

与《电子交易条例》（第553章）类似，《土地注册条例》（第128章）只包括了与财产有关的书面形式的契据、转让协议及其它文件，而《产权注册条例》（第219章）则明确规定了相关的文件应签署、盖章并交付。下一步将探讨修正《土地注册条例》（第128章）的可能性，以加强对数字抵押和权契证的监管；对《产权注册条例》（第219章）的修正以实现对相关文件进行电子处理的可能。

- **土地注册处的参与**

在前面讨论的产权所有权验证和抵押贷款计数子用例中，银行只能向DLT网络提交新完成的抵押贷款契据，而不是已有的契据。 《个人数据（隐私）保护条例》（第486章）规定了六条数据保护原则，其中也涵盖了一条个人数据的保护周期等。其中有一条规定，个人数据必须用于收集数据的目的或直接相关的目的，除非从数据主体获得自愿和明确的同意才能用于新的目的。因此，将所有现有抵押契约大量上传到DLT网络，将需要所有现有客户的实质同意，这几乎是不可行的。

在所有财产所有权和抵押贷款信息已按照财产所有权验证子用例所述逐一上传到DLT网络之前，银行必须使用替代方法从其他银行收集信息，而不能够直接从DLT网络检索信息。

即使土地注册处没有参与DLT网络，一旦抵押贷款申请获得批准，银行仍然可以向网络提供抵押信息和所有权信息。然而，数据库永远不会完整，因为不是每个交易交易都涉及到抵押贷款。

为了在DLT网络上提供抵押计数或全功能抵押贷款申请，土地注册处的参与是至关重要的。所以我们建议银行尽量让土地注册处投入到这项新科技的研究中来。

- **DLT的动态授权**

尽管数据总是可用于网络上的所有DLT节点，但是《个人数据（隐私）条例》的要求意味着节点控制器（例如银行）不应该在没有合法需要的情况下在网络上检索数据。抵押计数子用例要求银行在访问相关信息之前从数据主体获得授权。

为了符合上述要求，需要建立动态授权机制。我们的初步研究表明，可以通过使用数字身份在DLT中实现动态授权。 更多细节将在明年发表的白皮书的第二部分讨论。

- **DLT搜索功能**

关于抵押贷款计数子用例，如果所有抵押贷款契约都在DLT网络上可用，银行可以通过搜索DLT网络来获得单个申请人所欠的抵押贷款总数。但是，如前一章所述，交易记录按照账本区块链的时间顺序存储。随着时间的推移，更多数据存储在账本上，账本中的信息搜索会越来越耗时。

在DLT上实现高效搜索能力还需要进一步的研究。可能的解决方案包括在DLT之上构建索引，或者增强DLT协议以启用搜索功能。应科院将继续研究这个课题，并在下一阶段的白皮书中提供进一步的最新资料。

- **生态系统的准备**

为了充分利用DLT的特点，更广泛的生态系统必须完全准备就绪。例如，一个顺利运作的区块链抵押系统将需要所有有关方面的参与，例如鉴定人、律师和土地注册处等。我们观察到，一些业界利益相关者正积极地在其业务流程中采用新兴技术。然而，生态系统需要长时间才能成长并成熟，才能让技术改变我们的生活。

- **《个人数据（隐私）条例》的影响**

《个人数据（隐私）条例》的影响需要进一步研究。例如，虽然银行可以向DLT网络提供抵押贷款信息，但是每当银行想要提供所有权信息时，是否需要来自客户的同意，这点并不完全清楚。鉴于DLT网络中信息的不可变性，DLT网络如何满足《个人数据（隐私）条例》中关于数据保留期和个人对数据纠正对权利的问题尚待解决。目前没有官方工具用于搜索个人占有的房产数量。如果在DLT网络中存储抵押数据，则可以搜索所有权的详细信息。然而，需要探索与这些抵押数据搜索相关的法律方法以符合《个人数据（隐私）条例》的要求。

11.2 概念证明 – 贸易融资

简介

贸易融资是一个重要的商业工具。因此，它是银行提供的一项重要服务，作为中介，向参与全球供应链的进口商和出口商提供担保和促进资金流动。然而，为了降低商业风险，需要尽职调查，并严重依赖第三方的纸质文件，所以，毫无疑问，相关的过程需要耗费大量劳动力和时间。世界各地的各种联盟使用DLT进行了不同类型的概念证明工作，试图通过文件数字化简化进出口文件的手工程序，提高运作效率，减少错误并增加各方的便利性。该流程还旨在使公司的营运资本更可预测。与其他主要金融市场一样，香港的银行界面对同样的挑战。

鉴于此，金管局和应用科技业连同贸易服务商及五家参与银行，成立了一个DLT工作小组，探讨将DLT应用于贸易融资过程的可能性。

赊销贸易

传统上，银行通过提供流动资金、制造业筹资活动、防止欺诈和保证参与贸易交易的公司付款等服务在国际贸易中发挥着重要作用。近年来，出现了一种新趋势，即交易已从以跟单信用证为基础转变为以赊销贸易形式进行。赊销贸易意味着卖方在任何付款到期之前直接将货物交付给买方，而不依赖于银行出具的跟单信用证。促使企业将贸易从采用跟单信用证条款转向赊销贸易条款的一个主要因素是技术的进步，这使得通过互联网的市场参与者之间的通信和信息交换更加方便。

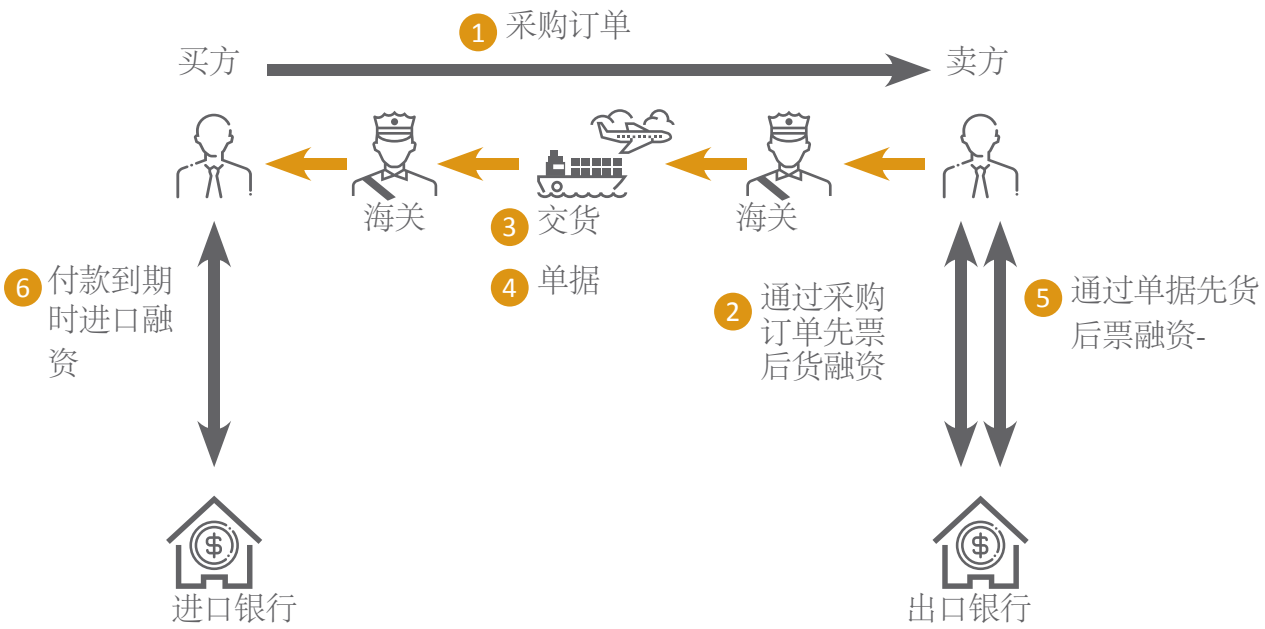
赊销贸易为银行提供了各种融资解决方案的机会，例如发票贴现、保理业务和买方担保融资。然而，赊销融资还意味着，与跟单信用证方式相比，由于缺乏第三方文件和交易状态的可见度低，银行存在更高的欺诈和洗钱的风险。

贸易融资 生态系统主要利益相关者

当前赊销贸易过程

从供应商到零售商的销售的简化的赊销贸易过程如下所示：

赊销贸易



流程说明:

1. 买方和卖方在特定日期和时间以赊销条款同意贸易交易。买方（例如零售商）创建采购订单（PO）并将其发送给卖方（例如供应商）以进行确认。

2. 卖方将PO提交给出口银行请求融资。出口银行根据风险确定是否同意先票后货融资，例如，PO未得到确认或重复融资。

3. 货物运到出口码头并由海关检查后，货物将运往进口国。在进口国海关查验后，货物交付给进口商。进口银行和出口银行都不能获得货物交付的状态。

4. 卖方通过文件快递员向买方提供单据、提单和其他运输单证。

5. 卖方通过提交单据要求出口银行要求先货后票融资。出口银行根据发生重复融资和／或欺诈交易风险程度，确定是否为卖方进行先货后票融资。

6. 6. 买方接受单据并要求进口银行进行进口融资。进口银行根据发生欺诈交易、重复融资或卖方融资的风险程度，确定是否为同意进口融资。

DLT应用于贸易融资

尽管交易双方从跟单信用证转向赊销支付条款，仍然需要银行服务来进行融资、风险缓解以及数据传输和匹配。银行需要对贸易交易的合同条款和卖方和买方之间的货物流动进行整体观察，以便在供应链中提供更好的价值服务，并在履行融资职责时降低风险。贸易融资概念旨在说明DLT提高贸易交易透明度的能力，并为三大领域的客户提供银行融资服务：

采购订单。采购订在赊销贸易中使用智能合约、跟踪贸易交易状态，以及将发票与PO匹配。

要加入DLT网络的文档

基于上述过程，以下三种类型的文件被认为对于贸易交易是最关键的，并且可用于DLT网络中：

1. 采购订单
2. 商业发票：在为采购订单出具的商业发票的范围内进行概念证明
3. 运输单证，可能包括提单、空运提单和海运单。

可以将其他交易文档（如装箱单和检验报告）的图像文件（jpeg，gif，tif格式）上传到DLT平台或再心存储库。尽管运输单据的所有权转让可以在DLT上进行，但并不包括在当前范围内概念证明工作。DLT平台上的传输文档仅用于信息共享，并提供有关货物运输状态的信息。

DLT特性测试

DLT的以下四个特性将在概念验证工作中证明：

1. **共享存储库** — 贸易交易中的多个利益相关者需要查看公共信息。
2. **多个编辑者** —贸易交易中的多个利益相关者采取需要记录和修改的行动。
3. **中间人（会增加成本和复杂度）** — 删除“中心机构”记录保管人或中间人有可能降低成本（例如费用）和复杂度（例如多重对账）

4. **互作用对时间敏感** — 减少延误符合商业利益，例如降低结算风险和增强流动性

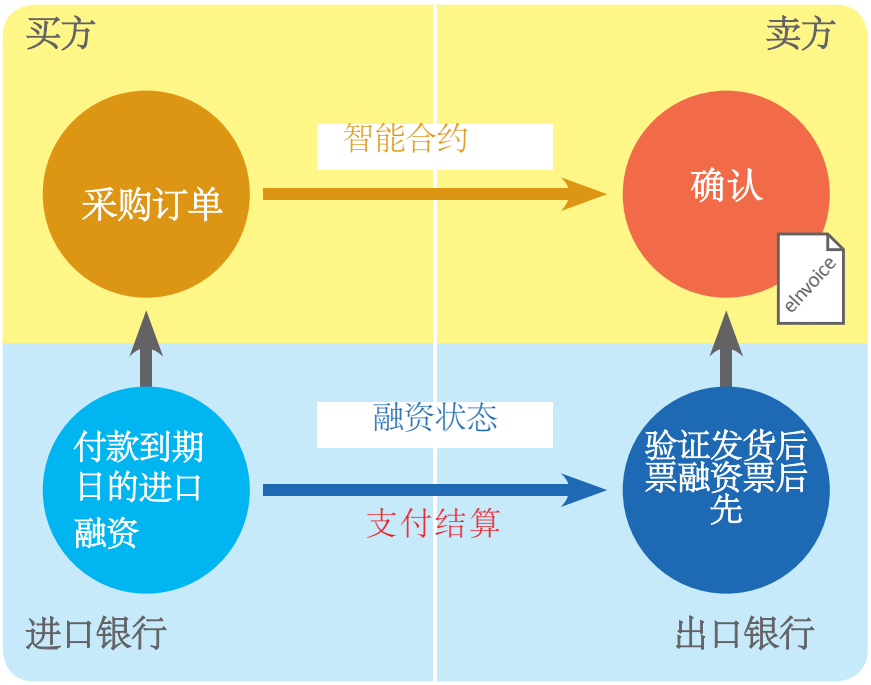
11.2.1 赊销贸易中的智能合约

基于PO的贸易交易通常是正式的。这是由买方和卖方商定并签署的，是执行交易的法律文件。有效的采购订单通常是设置贸易条款的关键文件，它们构成了关键信息，银行通过这些信息确定何时以及在多大程度上向买方和卖方提供融资。

贸易融资工作组建议制定一个智能合约模板，记录买方和卖方在赊销贸易条款下的买卖协议。基于DLT平台上记录的智能合约，买方、卖方及其银行可以提交交易文档并获得根据DLT平台规定许可的交易数据进行访问。根据"触发者"触发智能合约的条款，银行可以更快地为客户提供贸易融资。因此，提高了交易透明度，为客户提供融资的银行流程变得更快更有效。

要构建和测试的关键DLT智能合约功能：

1. 当买方创建PO，由卖方验证和接受时，形成智能合约，并且PO由买方和卖方两者数字签名。
2. 进口银行和出口银行都可以阅读采购订单。当满足智能合约的条件时，产生融资触发。这允许进口银行和出口银行在贸易交易过程中及时向买方和卖方提供资金。
3. 在付款到期日，智能合约提醒买家和进口银行履行付款义务，以及提醒卖家和出口银行结算出口融资。



智能合约工作流示例

当前流程不足:

- 采购订单没有标准结构
- 不能验证最新的采购订单版本
- 合同条款和对银行修订的可见度低
- 由于人为失误导致失误率高
- 效率低、成本高的，因为:
  - o 处理纸质文件
  - o 银行验证困难
- 欺诈风险

应用DLT实现的改进:

- 采购订单实现数字化和规范化
- 部署智能合约促使贸易自动执行
- 通过与海外DLT项目的合作促进跨境贸易融资
- 更快地向客户融资，并使得供应链上的阶段融资成为可能
- 降低融资风险，避免重复融资

11.2.2 跟踪贸易交易状态：货物流和资金流

跟踪贸易交易状态和货物流是赊销贸易的另一个挑战，因为与银行信用证不同，赊销贸易不需向银行提供第三方文件（如运输单据）。

贸易融资工作组提出的DLT解决方案是在DLT网络上存储和共享交易中的所有利益相关者都可以访问关键交易文件。此外，将在关键接触点收集来自物流服务提供商的多个数据馈送，以显示货物流的最新状态。存储在DLT网络上的关键信息包括由卖方报告的货物交付状态，来自物流服务提供商的运送信息以及来自银行的资金状况。此信息还将用于跟踪货物和资金的状态。结果，货物和交易中的资金流动的可见度将大大增强，并且降低欺诈交易或融资的风险。

要构建和测试的主要贸易交易状态跟踪功能：

1. 融资状态

   - 融资状况，即卖方的先货后票、先票后货融资，和买方的进口融资将在DLT账本上进行跟踪，交易中的所有利益相关者都可以看到，从而有助于防止重复融资。

2. 交付状态

   - 货物的交货状态将使用卖方提供的运输单据进行跟踪，实际的“货运”状态将基于从货运代理处收到的数据。

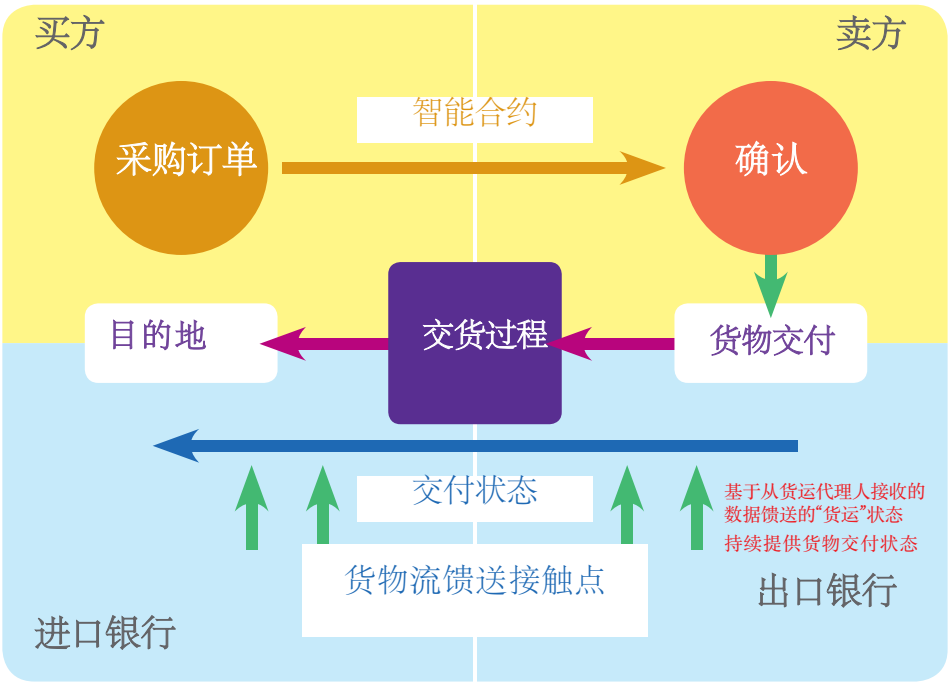
   - 货物到达目的港时交付状态变为“已交付”。

   - 使用来自承运商和/或货运代理商的数据馈送对货物流量进行额外跟踪，将降低欺诈性交易的风险。

3. 支付状态

   - 当买方接受发票和卖方提交的贸易文件时，更新付款状态的跟踪，并向卖方、进口银行和出口银行发出通报。

   - 买方在付款到期日的最后一笔付款将被监控。



更新装运交货状态示例

当前流程不足：

- 难以追踪:
  - 供应链（货物流、文件流和资金流）不同阶段

应用DLT实现的改进：

- 提高买方，卖方，银行和货运代理交换贸易文件、更新运输、交货和付款状态的能力
- 银行能够核实第三方的发票和其他文件，减少欺诈性融资；并能够在评估客户的融资请求时审查贸易交易的货物流动和融资状况（已完成的融资金额和性质）
- 增强采购订单 / 发票的融资状况的可视性，以减少双重融资的风险

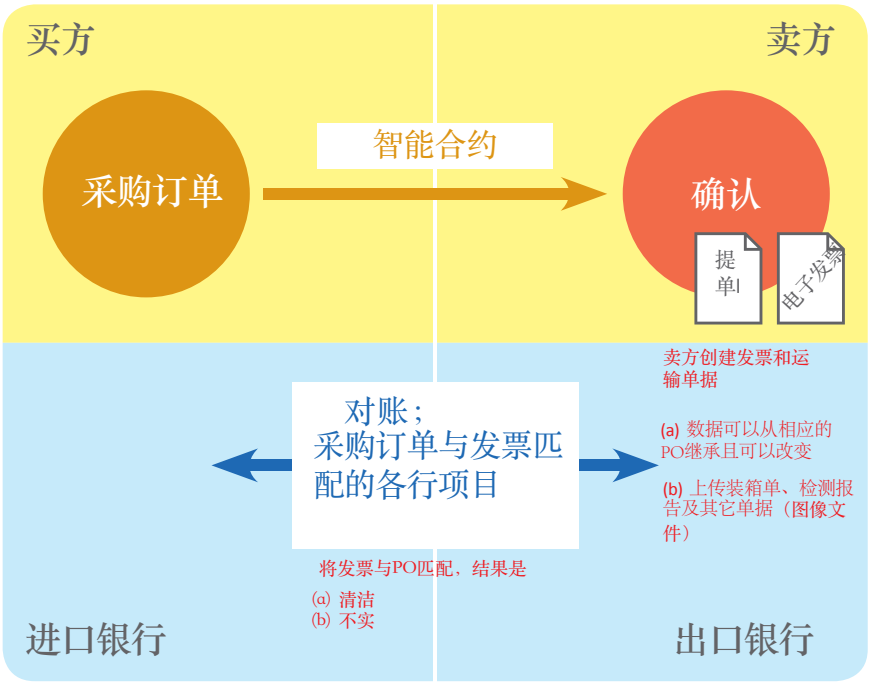
11.2.3 发票与采购订单的信息匹配

编制贸易文件所需的大部分数据来自采购订单。开具采购订单和发票时的数据继承可以减少手动准备发票的必要性以及减少失误。卖方提交的采购订单和发票（和其他贸易单据）的自动匹配可以识别差异并且向买方和融资银行提供早期报告。

要构建和测试的发票和采购订单匹配的主要功能：

1. 当卖方凭借采购订单创建发票时，DLT平台将发票和运输单据的各行项目详细信息与采购订单进行匹配。

2. 根据匹配结果的状态，“清洁”或“不实”，将从卖方向出口银行触发装运后资金融通请求，或者将向所有各方发送警报以进行对账。



发票与PO匹配示例

当前流程不足；

- 由于人工编制和对账产生的不一致和消耗劳动
- 可能出现单发票或或PO的双重融资
- 由于欺诈性贸易文件而导致贸易欺诈风险
- 允许部分装运时，需要额外努力检查未完成的采购订单项目

应用DLT实现的改进：

- 提交发票至账本，匹配发票与PO的详细信息
- 买家和卖家均可以与他们的银行共享经过验证的发票，以获得装运后资金融通（卖方）或进口融资（买方）

11.2.4 DLT的益处和可能面临的挑战

益处

DLT的防篡改性、透明性和可追溯性允许相关贸易数据被数字化并存储在DLT平台上，并与参与其中的利益相关者实时共享。赊销贸易融资过程采用DLT可以使所有参与合作伙伴的采购协议交易条款更加可视，并提高赊销贸易交易的透明度。这种透明的系统还可以使银行能够提供更好的客户融资服务。存储在DLT网络中的交易数据可以被验证和交叉检查，从而降低欺诈性融资的风险。最后但并非最不重要的是，贸易数据的标准化和数字化也有助于减少对账和人工错误。

可能的挑战

虽然DLT为改善业务和操作流程（如抵押贷款申请证明概念的案例所示）提供了一个很好的机会，但仍然存在一些可能阻碍技术成功应用的挑战。

管理由于DLT网络的数据共享、贸易融资行业的非标准化流程和程序以及跨境监管而产生的法律和监管问题（例如隐私问题），都是工作组下一阶段需要探讨的挑战。

截至2016年10月底，工作组正在开发用于测试各种DLT功能的原型。这个原型的开发已在金管局 - 科技创新中心开始进行。有关原型及其测试的更多细节将在稍后的白皮书中报告，计划于2017年下半年发布。

11.3 概念证明 – 数字身份管理

简介

客户进行银行开户、订阅银行服务或进行在线交易时，需要提供个人身份证明。客户的资产也与他们的个人身份绑定。如果个人身份信息未得到适当保护，身份盗窃可能导致财务损失和资产损失。此外，与个人身份相关的其他个人数据（例如与收入、负债、违约历史等相关的数据）构成了有用的信息，银行可以通过这些信息了解客户的财务状况和信用记录。政府和监管机构要求金融企业收集和检查客户信息，并遵守KYC规则和反洗钱指导方针。

与KYC和反洗钱有关的监管要求越来越多，这激励了金融机构寻找更低成本的机制来实施这些要求。此外，更便捷、用户友好的加载流程的需求正在增加以更好地服务于客户，尤其是海外客户。

爱沙尼亚在北欧启动了一个电子住宅项目，将数字身份服务应用于银行和咨询服务。电子住宅ID链接到居民的个人详细信息，并允许他们在使用金融服务时以数字方式证明他们的身份并进行数字签名。

在这个背景下，金管局和应科院与五家参与银行成立了数字身份工作组，研究将DLT应用于数字身份管理的可行性，以应对香港银行业面对的一系列挑战。该小组旨在确定主要问题和可能的解决方案，并确定DLT是否能够为数字身份管理提供具有成本更低的解决方案。

基于DLT的数字身份管理的潜在好处

DLT有可能让银行以更有效和更安全的方式共享身份信息。客户的记录和文档可以通过DLT平台实现数字化管理、在线更新和在银行间共享。这种安排将有以下益处:

- 客户不再需要为了KYC目的重复相同的流程，并向不同银行提交相同的个人信息;
- 身份验证过程所需的成本和资源可能会减少，因为这些信息将在DLT分类帐中很容易访问和共享;
- 对客户历史的检查可以有效地进行，因为客户的信息将在DLT账本中;和
- 会产生更好的客户体验。

工作组状态

截至2016年10月，数字身份工作组进行的概念验证工作仍处于非常初期的阶段。需要进一步研究以便寻找最佳方式从可靠的来源收集和验证个人信息、访问这些个人信息的认证过程，以及可能的法律影响。工作组旨在在本研究项目的下一阶段报告有关数字身份管理的调查结果和建议的详细信息。

附件 1 – 用例 – 抵押贷款证券 (由R3提供)

在会议中，另一个被关注的用例是抵押贷款证券（MBS），对该用例仍需要更加深入的研究。

传统的MBS基于银行在实际抵押贷款上的态度、对它们进行分析（例如创建池/分段），然后向市场发布特定分配，锁定特定的期限/风险篮。 这是MBS发行商的风险期。 在信贷危机之前，拍卖票据被用来资助这个过渡期。拍卖票据市场的枯竭是贝尔斯登公司衰落的主要原因之一。

可以设想在分布式账本上进行抵押事宜的一些场景：

1. *如果从个人借款人角度，抵押贷款是匿名的，但其他数据暴露在账本上，发行人可以采用抵押贷款证券而不持有它们。这将允许发行人融合池而不持有抵押贷款、提供MBS用于出售，并且根据需要组合标的证券，而没有仓储风险。*

2. *如果来自个人抵押贷款的个别原始现金流量记录在帐本上并可进行转让，MBS发行商可以从个别现金流量（例如优惠券和期限剥离）建立MBS模型，然后匹配他们需要的特定现金流量到现金流篮子的模型，而不是从个人抵押贷款进行上述行为。*

3. *或许最激进的"假设"情景将涉及创建智能合约，其中（a）将贷方与模型匹配，并且（b）通过类似于MBS的算法直接在另一端自动匹配到投资者的现金流量账本，破解了传统银行的中介作用和创建一个黑盒子代替传统的抵押贷款初级市场。*

然而，与其他证券的贸易生命周期一样，部分挑战将会协调参与这一进程的各方，包括：

- *原抵押贷款发行人。 最初提供抵押贷款的银行或贷款抵押机构*
- *抵押贷款服务商。 从抵押贷款持有者 处收集付款*
- *特殊目的工具(SPV). 包括抵押贷款，向投资者出具借贷票据*
- *票据持有者。 基于一些约定公式获取抵押贷款现金流*
- *票据保管人。保管人持有SPV出具的借贷票据*
- *收款账户开户行。 提供客户付款账户*
- *客户。抵押权人*

建议的解决方案是使用分布式帐本技术来管理从抵押贷款服务机构到财务小组再到业务和票据保管人的数据流。 结果将不再需要对账。

但是，仍然有一些待解决的问题，例如票据保管人的作用是什么。假设票据是在分布式账本上发行的，那么保管人目前执行的许多管理操作可以在分布式账本上完成。 托管人也处理付款。 可能分布式账本需要现金分类帐来完成这种业务，而这还需要很长时间。 这也符合中央银行发行的数字货币的主题，我们许多成员都对这个话题感兴趣。

附录 2 – 区块链在贸易融资中的应用 (由印度IBM研究院的Vishal Batra提供)

本文介绍了如何利用区块链技术促进贸易融资，以减少风险并为各方创造一个开放市场，从而促使各方通力协作、降低风险和确保交易安全的方法。

1. 区块链

区块链是一种新颖的点对点共享账本技术，没有任何中心系统或机构。区块链使各对等方/各当事方安全可靠地在所需的记录/数字资产上进行协作和处理，同时执行他们约定的条款和条件。每个对等体/当事方运行与其他区块链节点连接的区块链节点以创建网络，每个节点是相同的且保持完全相同的记录副本（在其本地账本上），并且统一地应用（执行）相同的交易规则集由此来确保/保证网络的每个节点上的每个交易的相同结果/最终状态。网络是私有的和有中心的，仅允许授权方/对等体加入网络并执行与其他方的交易。此外，只有网络上的协作方之间达成共识之后才可在账本上更新数据，这样就对账本防篡改性做了证明并且在协作中建立了信任和信度。共享账本还维护记录的更改历史记录（以前的值）以保留所有更新的踪迹 - 这就是在区块链上执行的交易审计功能。图1说明了区块链技术的概念。每个参与方都可在账本上看到相同的不可变的记录集，而这不要中心系统或机构。

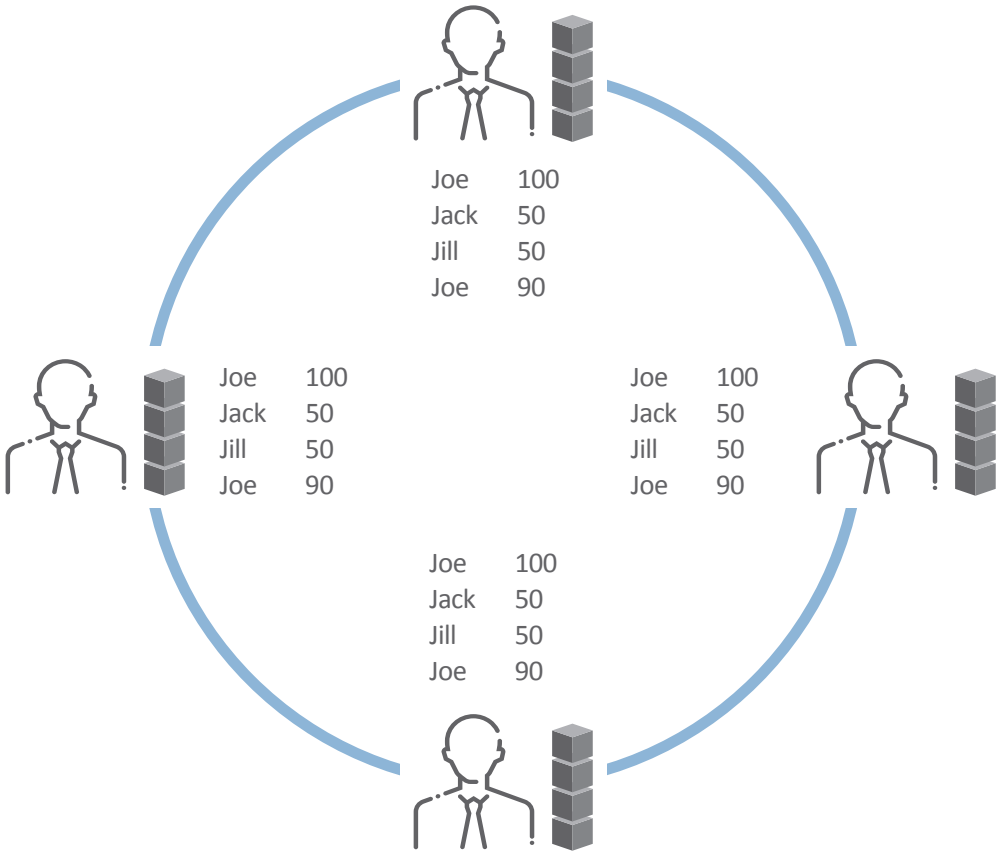


图 1. 图解区块链

2. 贸易融资

自1945年以来，国际贸易占全球国内生产总值的份额翻了两番，每年创造的贸易融资收入约为500亿美元。传统上，银行和金融机构通过提供信用证（L／C）- 银行代表买方（进口商）向卖方（出口商）提供的承诺/保证，在推动全球贸易方面发挥了至关重要的作用，如果卖方按照采购协议的规定向银行提交相关文件，然后银行将向卖方付款。因此，银行降低了风险并向出口商提供所需的担保，以可靠地与通常比较陌生的并处于外国管辖范围内的买方进行交易。最近，跨境电子支付变得更加容易，全球金融持续稳定，适用于贸易纠纷的仲裁和解决的国际贸易条约和法律的也比较统一和明确。赊销贸易融资，是一种基于信任而在商业合作中采取的一种方式，他们需要设立一个代理银行账户。只要全球市场条件趋于稳定，赊销贸易就会不断替代使用信用证的基于单据的贸易实务。然而，使用LC的基于单据的贸易融资在不稳定的市场中是优先采用的。因此，银行和金融机构及其系统和过程必须灵活有效地响应市场动态，以满足买卖双方贸易合同的复杂条款和条件。区块链为安全、可靠和有成本优势的贸易融资网络提供了所需的灵活性和灵活性。

3. 区块链下的贸易融资

区块链网络建立在银行/金融机构、买方（进口商）、卖方（出口商）、物流公司、海关等之间。每个实体是网络中的平等对等方/当事方，并且可以通过定义在它们之中的记录集，包括L／C和出口单据 - 发票、提单、装箱单等，以及各方可以通过对区块链的智能合约计算机网络智能合约计算机程序进行编码而利用这些文件和工作流程的交易集。例如，双方可以规定进口商首先在区块链上提交L／C应用程序，然后可以由其银行审查该L／C应用程序，并且只有在审核通过后，给定应用程序才能生成L／C并将其交给出口商的银行以进行审查、审批。在出口商银行批准后，L／C将不可撤销且在各方之间具有约束力，出口商可以安全可靠地配送订单。区块链提供对记录达成的共识和不变性，并确保只有被授权方能够在其上执行允许的交易，从而消除记录和冲突上的不一致和差异的任何可能性。

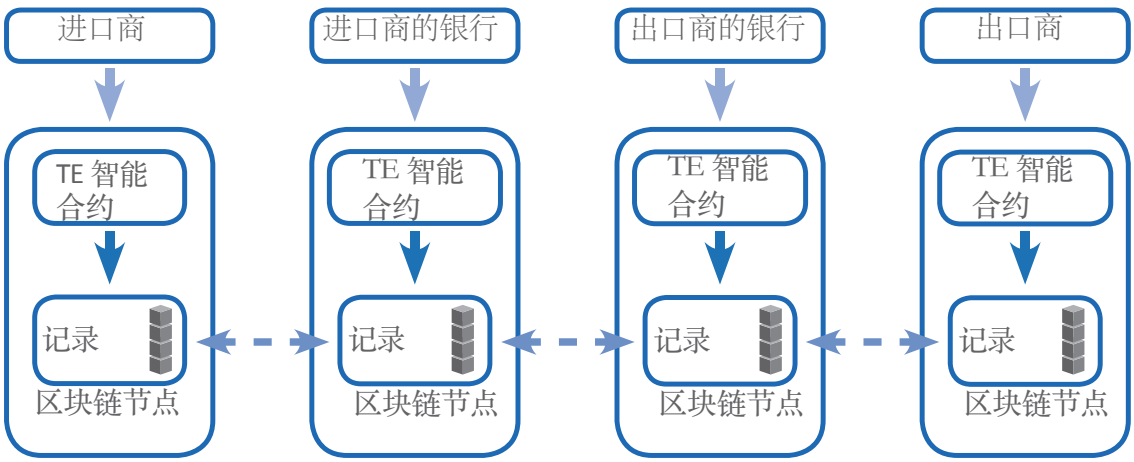


图 2. 贸易融资区块链网络

4. 贸易融资市场

在互联网和电子商务的时代，买卖双方在网上会晤和谈判。在国际贸易中，不同国家的买卖双方可能没有见面。因此，银行降低了未知方之间的风险。然而，银行必须与外国地区的其他银行建立渠道和联盟，以降低风险并实现国际贸易。即使在每个市场都占据领先地位大银行，也是一笔不小的开支。在不同法律下运作的其他银行在全球建立此类渠道和联盟，确保当地国家的法律合规需要复杂的程序和大量的成本支出。结果是银行与每个地理区域中只有几个主要/大型银行形成联盟和合作伙伴关系。因此，较小的银行和金融机构必须通过其代理银行进行贸易融资，其进一步将交易给当地领先银行以完成端到端交易。随着这种中间银行的数量增加，进口商和出口商的总交易成本也会增加。

区块链技术可以用于创建一个全球贸易融资市场，并通过动态地发现进口商的银行和出口商的银行之间具有最少数量的中介的最具成本效益的信任路径，进而降低交易成本。基于区块链的市场允许各种规模的银行和金融机构加入全球贸易融资市场并提供服务。这些实体与他们信任的网络上的其他实体连接，从而定义它们之间的信任链接。对于每个全球贸易，区块链发现进口商的银行和出口商的银行之间的最佳信任路径，从而消除银行与每个地理位置的多个银行形成直接联盟和协议的要求。网络上的每个实体公布其合同条款和费用。区块链协议挑选信任路径中的条款和条件与其他条款和条件相匹配的实体以及进口商和出口商指定的条款和条件，同时确保将整体交易成本保持最小。这些实体作为全球贸易金融区块链网络的做市商为贸易融资提供信任和促进流动。

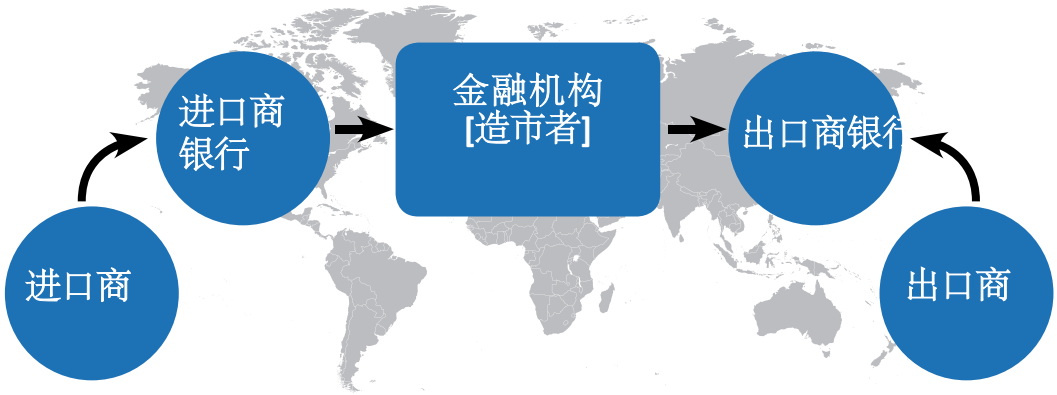


图 3. 基于区块链网络的贸易融资市场

5. IBM区块链技术及方案

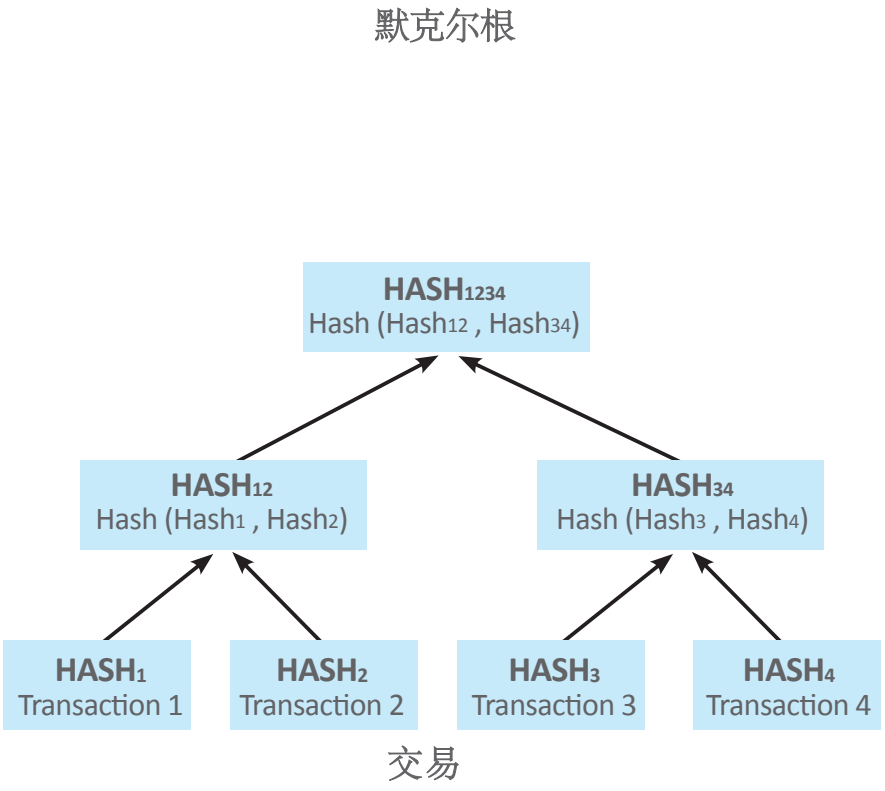
根据业务需求和用例，IBM和合作伙伴正在部署企业级的可编程、安全、有中心的和可审计，且允许在区块链上实施定制和可扩展解决方案的区块链结构。区块链构造-超级账本（https://www. hyperledger.org/）是Linux基金会下的一个面向所有人开放的开源项目。 IBM还在安全的SoftLayer云上部署了其所拥有的超级账本节点。

技术说明 (I) – 默克尔树

默克尔树以拉尔夫·默克尔的名字命名，他获得了哈希树概念的专利权。默克尔树是一种二叉哈希树，是一种合并一组叶节点的有效方法。每个非叶节点用其子节点的哈希标记。

在DLT中，使用默克尔树来合并区块内的交易。每个交易由哈希值表示。交易哈希值作为叶节点附加到默克尔树的底部。然后，从叶节点往上推，直到到达树的顶部，这一代就剩下一个哈希了，我们把它叫做默克尔根（Merkle root）。当使用SHA256哈希时，所有节点和默克尔根的哈希值为32字节长。

如果为了证明区块中交易是否存在，不需要知道该区块内的所有交易的哈希值。为了证明其在包括N个交易的区块内的存在，所需要的是log2（N）个哈希值和执行相等数量的哈希运算：在每个级别进行一个哈希操作，在下一个步骤重复水平向上推，直到到达树根（如下图所示）。如果计算的根哈希值与已知根值相同，则证明交易的存在。这很明显加快了验证交易的速度，同时减少了证明数据块内特定交易的存在所需的区块信息量（参见下图）。



一个含有四次交易的默克尔树中，底部叶子节点是各自交易的哈希值。每组哈希值再进行哈希运算，依次往上推，直到只剩下一个哈希，我们称之为默克尔根。
为了证明区块中存在默克尔根的值为 $HASH_{1234}$的transaction 4，只需知道$HASH_3$ and $HASH_{12}$的值即可。

默克尔树用于表示区块中的交易，计算出的默克尔根村春在区块的顶部。

以太坊使用称为Merkle-Patricia树（简称为Patricia树）的树结构。使用这种结构是因为以太坊DLT不仅需要存储不可变的交易历史，而且还需要存储通过合同执行生成可用Patricia树表示的状态信息。

技术说明(II) – 图示: 利用SHA256哈希算法的挖掘工作量证明

区块数据:
m0-rf9falgvoaiujrewmr89u12394=-19324132432490-132m51m4353ti3m-0223;2-0mpir,fbv0-p[da,;baewtr0-weryg;qwytgr2y0-apfd,a;gf0-afasodfasd9foas-o9fas0-fpaqw,reqk3=0aeg=0-as9df-a9=-g09sdhfios9ns9f=0-or4w,513259=0-9326t4-ow0f=-n0sfn-dno9=0-kr,v.a,fd v] fm= o-f[pae0fo 3-v8ap[3evl;dfva9ib[32]Fsbd9akreopbf,324mn1jvs

目标:
找到{Data + Nonce}的SHA256哈希，使得哈希的前12位都是0。

矿工-A

哈希运算结果

Nonce	Hash
0:	736fcfa89db20b8f1...
1:	7fdc40dd3a03fe9b9...
2:	bcfbd8deff2d5f616...
3:	64ae0630a91821ea4...
4:	288bd40ab85e9216a...
5:	1984d6d9b141787cd...
6:	9fc9f88659a222716...
.	
122:	00cd22ac7ea221ddc...
.	
4000:	0792f2654d208824a....
.	
.	
.	
5203:	00053e801178649e4....

矿工-B

哈希运算结果

Nonce	Hash
0:	736fcfa89db20b8f1...
1:	7fdc40dd3a03fe9b9...
2:	bcfbd8deff2d5f616...
3:	64ae0630a91821ea4...
4:	288bd40ab85e9216a...
5:	1984d6d9b141787cd...
6:	9fc9f88659a222716...
.	
122:	00cd22ac7ea221ddc...
.	
4000:	0792f2654d208824a....

工作量证明

1. 矿工A和口感B都开始需要大量计算的哈希运算，并不断重复，以找到满足目标要求的nonce数
2. 矿工A已经进行了5204次哈希运算，并找到了满足目标要求的nonce值：5203
3. 此时，矿工B刚进行了4001次计算，尚未找到合适的nonce值
4. 矿工A胜出。他将他的发现在网络中广播并会受到工作量证明奖励。

验证工作量证明

网络中其他人不需要区执行5024次哈希运算，只需要对{Data + “5203”}进行 SHA256哈希运算，看是否能得到哈希值为00053e801178649e4f....的结果。

技术说明(III) – 关于平台和应用部署思考

不同的DLT平台具有不同的特性，对开发应用程序也有不同的要求。本节介绍一些主要的DLT特性，并列举一些支持它们的常见DLT平台的示例。 在设计和部署DLT应用程序时应思考下列信息。 例如，一般公众参与的应用通常部署在无中心的DLT平台上。 针对较小节点群组的应用程序更适合于有中心的DLT平台。

1. 不受信任节点的参与

DLT平台可以部署在私有或公共网络中。 不管它们部署在何处，参与DLT交易和操作都是由DLT平台的设计决定的。 无中心的DLT，也称为公共DLT，允许任何人作为用户或矿工参与。 相比之下，有中心的DLT，被称为私有DLT，需要对参与的成员资格控制。

类型	接受非可信节点 (无中心的 DLT)	仅支持受信任的节点 (有中心的 DLT)
示例	比特币	瑞波币
	以太坊	超级账本
		Corda

2. 初步应用

一些DLT平台可支持不同的应用，而其他DLT平台是为特定类型的应用定制而来。这两种方法各有千秋。前者提供更具灵活性，而后者可以为特定类型的应用程序提供更高的效率和更丰富的功能。

它们的功能主要分为两种：不可变账本记录和智能合约。 每项功能还可以具有进一步的细化。

类型	账本记录	智能合约
示例	*比特币：支付*	*比特币：支付合约*
	以太坊：支付	*以太坊：通用应用程序*
	瑞波币：结算	*超级账本：通用应用程序*
		Corda:*金融应用程序*

3. 数据库结构

DLT的应用从Bitcoin开始，它在包含交易记录的区块链上构建其分布式数据库。 一些较新的DLT平台与其他数据结构共同构建数据库，其原因是实现更好的性能、更加确保隐私和及更好的进行控制。

类型	区块链	非区块链
示例	比特币	**Corda**
	以太坊	瑞波币
	超级账本	

4. 共识机制

已经设计了各种共识算法并将其并入不同的DLT平台。这些算法主要有两种类型：（a）基于证明的共识，和（b）容错共识。 在无中心的DLT网络中使用基于证明的共识算法，矿工证明其可信度以便向区块链添加新区块。 在有中心的DLT中的验证节点不需要证明其可信赖性，因为它们是预先限定的。 相反，他们均采取容错共识，以确保其管理下的账本的所有可复制副本的一致性。

类型	基于证明	容错共识
示例	比特币： *SHA256 哈希工作量证明*	**超级账本:** 不同共识，包括 PBPT（实用拜占庭容错共识）
	以太坊: *Ethash哈希工作量证明*	**Corda:** 个人交易层面而非国际层面的不同共识
		瑞波币： *拜占庭，利他主义，理性 (BAR) 模型共识*[4]

5. 加密数字货币

一些DLT平台支持本地加密货币，因此可以直接用于支付交易。其他DLT平台不支持，而是支持账本记录和基于智能合约的应用程序。可以为这样的平台开发应用程序，以使得它们能够兼容新的加密货币。

示例	有本地加密货币	无本地加密货币
类型	**比特币:** *比特币 (BTC)*	超级账本
	以太坊: *以太币 (ETH)*	**Corda**
	瑞波: *瑞波币 (XRP)*	

6. 透明度

无中心的DLT平台为节点提供全透明度，他们可以访问整个账本及其包含的交易。有中心的DLT平台设立了不同程度的交易访问控制。对交易的访问可以仅限于交易的参与者。 交易也可以被加密，只有相关参与者能够以普通形式访问交易。一些有中心的DLT平台还可以限制智能合约对验证节点已选择的子集进行验证和执行。

类型	对所人开放	经允许的有限访问
示例	比特币	超级账本
	以太坊	**Corda**
		瑞波[25]

7. 脚本语言图灵完备

DLT平台中的智能合约是用计算机语言编写的。主要分为两种：图灵完备和非图灵完备。图灵完备语言灵活度较高，支持起草复杂的合同条款。 非图灵完备语言对复杂合同设置更多的控制，并且更适合于特定种类的合同应用程序。

类型	非图灵完备	图灵完备
示例	比特币：脚本	以太坊: *Solidity*
		Corda: *Java和其他*
		超级账本: *Golang和其他*

References

[1] See "Bitcoin: A Peer-to-Peer Electronic Cash System" at https://bitcoin.org/bitcoin.pdf
[2] See "Command line options" at https://github.com/ethereum/go-ethereum/wiki/Command-Line-Options
[3] See "Corda: An Introduction" at https://static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/t/57bda319ebbd1acc9c030abd/1472045850269/corda-introductory-whitepaper-final.pdf
[4] See "Hyperledger Whitepaper" at http://www.the-blockchain.com/docs/Hyperledger%20Whitepaper.pdf
[5] See "Enabling Blockchain Innovations with Pegged Sidechains" at https://blockstream.com/sidechains.pdf
[6] See "Bitcoin: A Peer-to-Peer Electronic Cash System" at https://bitcoin.org/bitcoin.pdf
[7] See "Corporate website of Ethereum Foundation" at https://www.ethereum.org/
[8] See "Bitcoin Vs Ethereum: Driven by Different Purposes by Prableen Bajpai, CFA (ICFAI)" at http://www.investopedia.com/articles/investing/031416/bitcoin-vs-ethereum-driven-different-purposes.asp
[9] See "Hyperledger Whitepaper" at http://www.the-blockchain.com/docs/Hyperledger%20Whitepaper.pdf
[10] See "R3" at https://r3cev.com
[11] See "Introducing R3 Corda" at https://r3cev.com/blog/2016/4/4/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services
[12] See "Ripple – Key Feature" at https://ripple.com/technology
[13] See "XRP Portal" at https://ripple.com/xrp-portal
[14] See "About R3" at http://r3cev.com/about/
[15] See "The Ripple Protocol Consensus Algorithm" at https://ripple.com/files/ripple_consensus_whitepaper.pdf
[16] See "What is the Bitcoin Block Size Debate and Why Does it Matter?" at http://www.coindesk.com/what-is-the-bitcoin-block-size-debate-and-why-does-it-matter/
[17] See "Protect your privacy" at https://bitcoin.org/en/protect-your-privacy
[18] See "Protocol Specification" at https://github.com/hyperledger/fabric/blob/master/docs/protocol-spec.md
[19] See "Bitcoin worth $72 million stolen from Bitfinex exchange in Hong Kong" at http://www.reuters.com/article/us-bitfinex-hacked-hongkong-idUSKCN10E0KP
[20] See "Contingency Plans" at https://en.bitcoin.it/wiki/Contingency_plans.
[21] See "Contingency Plan" at https://bitflyer.jp/en/contingency
[22] *Lis pendens* is a written notice that a lawsuit has been filed with respect to a property, concerning the ownership of the title or a claim in it
[23] See "Architecture of the Hyperledger Blockchain Fabric" at https://www.zurich.ibm.com/dccl/papers/cachin_dccl.pdf
[24] See "A Protocol for Interledger Payments" at https://interledger.org/interledger.pdf
[25] See "Key Features" at https://ripple.com/technology/