DLT 相关技术调研

一、DLT 定义

DLT（Distributed Ledger Technology，分布式账本技术）是一种通过分布式网络记录和共享数据的技术，允许多个参与者在没有中央权威的情况下共享、验证和存储数据。其核心在于通过分布式的节点网络来维护账本，每个节点都拥有完整或部分账本副本，从而实现数据的高度一致性和可靠性，可移除当前市场基础设施中的效率极低和成本高昂的部分。

二、DLT 发展历程

DLT 的某些最早形式始于古代。历史学家报道说，在古罗马，有一个分布式分类帐，允许其公民在帝国的任何地区进行购买。该分类帐有助于刺激整个帝国的经济活动，并帮助罗马取得了历史地位。

DLT 的数字版本早在 1991 年就开始出现。此时，出现了当今众所周知的 DLT 的第一个概念。第一个 DLT 仅仅是两个名为 Stuart Haber 和 W. Scott Stornetta 的研究人员在一篇论文中写的一个概念。在他们的论文“ 如何为数字文档加上时间戳，这两个讨论的用于验证数字文档的创建和修改的过程 ”中，数字 DLT 的基础开始成形。

2002 年,DavidMazières 和 Dennis Shasha 在他们的工作中建立了这一概念。两位创新的开发人员介绍了“ 从称为 SUNDR（安全不可信数据存储库）的拜占庭式存储多用户网络文件系统构建安全文件系统 ”的概念。该文档是第一个讨论使用块组织事务的可能性的文档。

在 2005 年，尼克·萨博（Nick Szabo）著名地提出了最早的一种数字现金形式——比特黄金。他的建议当时是革命性的。它引入了前所未有的概念，例如客户难题功能和工作量证明功能。这些概念中有许多进入了比特币的核心编码。

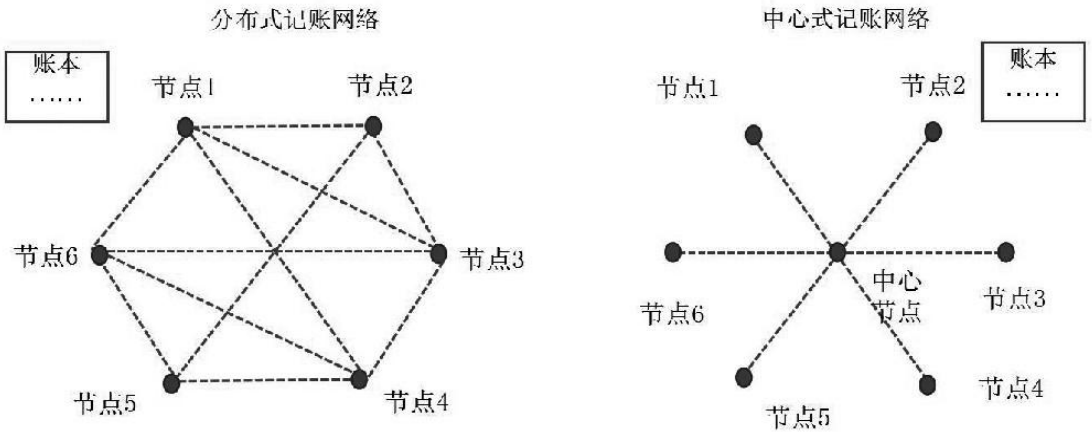
2009 年的比特币改变了一切。将区块链网络引入 DLT 领域是一项巨大的进步。这意味着历史上首次可以使用可靠且可验证的数字货币。

2015 年，区块链平台 Iota 推出了 DLT，该 DLT 可以利用物联网（IoT）进行验证。物联网由世界上每一个智能设备组成。在这种新型的 DLT 中，称为 Tangle 的协议将使全球数十亿智能设备能够验证网络状况。本质上，这种发展创造了目前最大的 DLT。

R3 的 Corda DLT 的引入是 DLT 的另一项重大发展。重要的是，Corda 不是区块链。R3 的新系统利用可插拔的公证者达成共识。有趣的是，单个 Corda 网络可能包含多个公证人，这些公证人使用各种不同的算法提供保证。这样，Corda 不会依赖于任何特定的共识算法。

三、DLT 主要特点

1. 去中心化：DLT 不依赖单一中心化机构来维护和验证数据库。数据的处理和存储分布在网络的多个节点上，增强了系统的抗故障能力和抵御篡改的能力。



2.透明性：网络中的所有参与者可以访问 DLT 数据库的副本，并验证记录的真实性。这提高了数据的透明度，同时保护了用户的隐私。

3.不可篡改性：一旦数据被添加到 DLT 中，就无法被更改或删除。每个记录都是不可逆的，这为数据的真实性和一致性提供了保证。

4.共识机制：DLT 使用共识算法来在网络节点之间就数据的准确性和顺序达成一致。这确保了分布式数据库的一致性和完整性，即使在存在恶意节点的情况下也是如此。

四、DLT 重要性

1. 增强安全性：加密技术和去中心化存储提高了个人信息的安全性。分权是 DLT 整个概念的基础。这些网络更加安全，因为它们删除了任何集中式攻击媒介。在 DLT 网络中，风险从一个集中目标转移到数千个较小的媒介。由于这些较小的节点没有中央管理机构等大量有价值的资产，因此它们遭受重大攻击的可能性较小。此外，DLT 利用高科技安全性来确保其网络保持纯净。输入恶意或错误数据的节点将立即从网络中驱逐。该策略有助于简化整个共识过程。

2.提高效率，提升用户体验：通过去除重复的身份验证步骤，加速了客户的注册和验证过程。客户可以轻松地控制自己的信息，并在不同机构间重复使用已验证的身份，提高了用户体验。

3.降低成本：DLT 的不信任性质使它们成为寻求安全网络解决方案的公司的有吸引力的替代方案。诸如区块链网络之类的 DLT 消除了对第三方验证系统的需求。由于这些系统中的每一个都会为每次交易增加更多的成本和时间，因此消除它们会大大提高效率。公司了解这些网络的点对点性质使它们比集中式系统更易于运行。

4.防篡改，使交易更透明：没有中间机构的参与，交易信息都清晰可见，保证账目数据的真实性和安全性。

5.可扩展性提高:分布式存储使数据分散存储在不同服务器内,增加了存储节点。

五、DLT 工作原理

可以通过一个假想的简化例子来详细探讨:一个基于 DLT 的供应链管理系统。这个系统旨在记录和追踪产品从生产到消费者的每一个环节,确保产品的真实性和供应链的透明度。

步骤 1:初始化网络

建立参与者节点:供应链中的每个参与方(例如,原材料供应商、制造商、物流公司、零售商)都在 DLT 网络中设置节点。每个节点保持一个账本的副本。

定义共识机制:选择一个共识机制(例如,权益证明 PoS)来协调不同节点之间的数据一致性,确保账本的更新能在整个网络中被验证和接受。

步骤 2:记录交易

发起交易:当原材料从供应商发送到制造商时,这个事件作为一个交易被记录下来。交易信息包括原材料的类型、数量、发送和接收方的标识等。

签名验证:交易由发起方用其私钥签名,网络中的其他节点可以使用发起方的公钥来验证签名的有效性。

步骤 3:达成共识

交易验证:所有的节点使用共识机制来验证交易的合法性。例如,在 PoS 机制中,持有更多货币的节点可能有更大的权力来验证交易。

创建新的记录:一旦交易被验证,就会被添加到新的数据块中。这个块还包括前一个块的哈希值,创建一个不可更改的链。

步骤 4:同步账本

广播和验证:新创建的块被广播到网络中的所有节点。其他节点验证新块的合法性(包括交易的有效性和块的哈希值)。

账本更新:一旦验证通过,每个节点更新其账本副本以包括新的块。这样,网络上的每个节点都保持着完整、一致、更新的账本。

步骤 5:查询和审计

透明度:任何供应链参与者可以查询 DLT 账本,以追踪产品的历史和状态。消费者也可以访问这些信息,以验证产品的真实性。

不可篡改性:由于每个块都包含前一个块的哈希值,任何对已有块的篡改都将导致后续所有块的哈希值不匹配,从而被网络检测到。

使用的技术和工具:

加密技术:非对称加密和哈希函数用于确保交易的安全和数据的不可篡改性。

智能合约:可以用于自动化供应链中的某些流程,如自动付款给供应商一旦货物交付验证。

分布式数据库技术：确保账本在网络中的每个节点上都有一致的副本。

六、区块链技术

区块链技术是一种革命性的分布式数据库技术，它通过密码学算法，将数据以区块的形式链接起来，形成一个不可篡改、去中心化的数据库系统。每个区块都包含一定数量的交易信息，并通过加密技术保护，确保数据的安全性和完整性。

区块链技术具有去中心化、不可篡改、可追溯等特点，这些特点使得区块链在金融、供应链、物联网等领域有广泛应用。例如，在金融领域，区块链可以用于跨境支付、数字货币、智能合约等，提高交易效率和安全性；在供应链领域，区块链可以实现全程追溯和防伪溯源，提高供应链的透明度和效率；在金融方面，区块链技术可以用于跨境支付，如瑞波网络利用区块链技术实现了低成本、实时的国际支付服务。此外，区块链还能应用于数字货币，如中国的数字人民币，它基于区块链技术，旨在替代部分现金流通，提高了支付效率。

1. 核心概念

- 区块：区块是区块链的基本单元，包含交易数据、时间戳和前一个区块的哈希值。
- 链：区块通过哈希值链接，形成一条链，确保数据的连续性和不可篡改性。
- 分布式账本：数据存储在多个节点上，而非单一中心化服务器，确保去中心化和透明性。
- 共识机制：通过共识机制如确保所有节点对账本状态达成一致。

  1）工作量证明（PoW）

  节点通过解决复杂数学问题竞争记账权，比特币采用此机制。

  2）权益证明（PoS）

  节点根据持有的代币数量和时长获得记账权，以太坊 2.0 采用此机制。

  3）委托权益证明（DPoS）

  持币者投票选出代表节点负责记账，EOS 采用此机制。
- 加密技术：使用加密算法保护数据安全，防止未经授权的访问和篡改。

2.运行机制

区块链的运行机制涉及多个关键步骤，包括交易生成、交易验证、区块创建、共识机制和链的扩展。

示例：比特币区块链

1.交易生成

场景：A 想向 B 发送 1 个比特币。

步骤：

A 创建一笔交易，包含输入（她的比特币地址和余额）、输出（B 的比特币地址和发送金额）和签名。

交易被广播到比特币网络中的所有节点。

2.交易验证

步骤：

网络中的节点收到交易后，验证其有效性，包括签名、余额和格式。

如果交易有效，节点将其放入未确认交易池（mempool）。

3.区块创建

步骤：

矿工从 mempool 中选择多笔交易，打包成一个新区块。

新区块包含区块头（版本号、前一个区块的哈希值、时间戳、难度目标等）和交易列表。

4.工作量证明（PoW）

步骤：

矿工通过解决复杂数学问题（寻找特定哈希值）竞争记账权。

第一个找到有效哈希值的矿工将新区块广播到网络。

5.区块验证与链的扩展

步骤：

其他节点收到新区块后，验证其有效性，包括交易和哈希值。

如果区块有效，节点将其添加到区块链中，形成新的链顶。

6.奖励与确认

步骤：

成功挖矿的矿工获得区块奖励（新生成的比特币）和交易手续费。

交易被包含在区块中后，随着后续区块的增加，确认数增加，交易被视为更安全。

3.区块链发展历程

区块链实际上是由特殊底层技术构建的分布式账本的一种形式，起源于中本聪先生在 2008 年的文章 Bitcoin:a peer-to-peer electronic cash system，是点对点技术(P2P 技术)、密码学、智能合约等现有技术的重新组合，之后便广受关注。

区块链作为虚拟货币的底层技术，分 3 个发展阶段：

（1）区块链 1.0 阶段 数字货币，以比特币为代表，随后还产生了莱特币、以太币等数字货币。认为区块链这样一个全新的、去中心化的数字支付系统，无障碍、低成本的运营冲击了传统的金融体系

（2）区块链 2.0 阶段 可编程化区块链，以功能强大的智能合约开发和应用为代表。比特币的底层技术——区块链技术很好地解决了智能合约中的技术难题，恰好提供了可信环境。这一阶段的标志性产物是以太坊[18～21],一个开源的具有智能合约功能的公共区块链平台，应用范围也开始从单一的数字货币领域扩展到其他金融领域

（3）区块链 3.0 阶段 高级智能合约，是超越货币、金融范畴的区块链应用，致力于为各行业提供去中心化方案，如物联网、医疗、物流等领域。这一阶段区块链技术的去中心化和共识机制发展到了新的高度

2013 年，一名以色列希伯来大学的学者首次将 DAG(directed acyclic graph)概念作为共识算法引入到区块链项目中来，然后有学者用 DAG 结构来存储块，打破了区块的概念，实现了区块链的并发打包和执行。面对区块链吞吐量低、延迟高等局限性， Baird 在 2016 年开发了一种新技术，名为 Hashgraph, 并声称其

可以做到真正的 blockless。此外，还有 Holochain、fruitchains 等架构。

4.区块链技术的优势

1.去中心化

区块链不依赖中心化机构，数据由多个节点共同维护，增强了系统的抗风险能力。

2.透明性与不可篡改性

所有交易公开透明，且一旦记录无法篡改，提高了数据的可信度。

3.安全性

通过加密算法和共识机制，区块链能够有效防止数据篡改和攻击。

4.降低中介成本

去中心化减少了中间环节，降低了交易成本和时间。

5.创新应用

支持智能合约、去中心化金融（DeFi）、NFT 等创新应用，推动了新商业模式的发展。

5. 区块链技术面临的痛点

1.扩展性问题

区块链的交易处理速度较慢。例如，比特币每秒只能处理 7 笔交易，以太坊每秒约 30 笔，远低于传统支付系统（如 Visa 每秒处理数千笔）。

2.高能耗问题

采用工作量证明（PoW）机制的区块链（如比特币）需要大量计算资源，导致能源消耗巨大。

3.交易成本高

在网络拥堵时，交易手续费可能大幅上涨，影响用户体验。

4.隐私保护不足

区块链的透明性可能导致用户隐私泄露，尤其是在金融和医疗等领域。

5.监管与合规问题

区块链的去中心化特性与现有监管框架存在冲突，可能导致法律风险。

6.技术复杂性

区块链技术门槛较高，普通用户和企业难以快速上手。

7.跨链互操作性差

不同区块链之间的数据互通和资产转移仍然困难，限制了生态系统的扩展。

6.针对痛点的潜在解决方案

1.扩展性问题

分层扩容：采用闪电网络（Lightning Network）等二层解决方案，将大量交易转移到链下处理，减轻主链负担。

分片技术：以太坊 2.0 通过分片技术将区块链分成多个分片，并行处理交易，提高吞吐量。

侧链：通过侧链处理部分交易，主链只记录最终结果。

2.高能耗问题

共识机制优化：采用权益证明（PoS）、委托权益证明（DPoS）等低能耗共识机制，替代工作量证明（PoW）。

绿色挖矿：推广使用可再生能源进行挖矿，降低能源消耗。

3.交易成本高

动态手续费机制：根据网络拥堵情况动态调整手续费，优化交易优先级。

批量交易：将多笔交易打包处理，降低单笔交易成本。

4.隐私保护不足

零知识证明（ZKP）：通过零知识证明技术（如 Zcash）实现隐私保护，验证交易有效性而不泄露具体信息。

隐私计算：结合多方安全计算（MPC）等技术，保护用户数据隐私。

5.监管与合规问题

监管科技（RegTech）：开发符合监管要求的区块链解决方案，例如可审计的隐私保护技术。

沙盒机制：政府通过监管沙盒支持区块链创新，同时确保合规性。

6.技术复杂性

开发者工具：提供更友好的开发工具和文档，降低开发门槛。

教育培训：加强区块链技术的人才培养和普及教育。

7.跨链互操作性差

跨链协议：开发跨链协议（如 Polkadot、Cosmos），实现不同区块链之间的资产和数据互通。

标准化：推动区块链技术的标准化，促进不同链之间的兼容性。

7.区块链与 DLT

DLT 是区块链的四大核心技术之一。区块链的分布式账本是一种去中心化的分布式数据库，与传统巨头使用的中心化数据库相比，区块链的分布式账本将账本的维护权力分散到每个人手中，防止数据被中心化巨头控制或 滥用。分布式账本提高了数据的可靠性、服务的可用性和异地容灾性，同时降低了成本。

虽然区块链是 DLT 的最著名实现，但 DLT 并不仅限于区块链。区块链特指一种以区块为基本数据单元，通过链式结构连接的 DLT 实现。而 DLT 包括了更广泛的技术和架构，如有向无环图（DAG）等，这些技术在处理速度、扩展性等方面有不同的优化。

区块链是完全公开的，这意味着任何人都可以查看交易历史并参与这些操作，区块链是一个不需要访问权限的网络。任何人都可以成为验证者（也称为节点或矿工），只需要他们拥有相关技术知识和足够强大的硬件。而部分的分布式帐本，只有选定的参与者才能访问和使用相关网络的功能，通常是特定的企业或组织所组成的联盟，透过分布式帐本共享的资讯是为了提升运作效率，但其中仍有许多机密是无法透露的，这在某方面也限制了部分分布式账本的应用及规模。

七、DLT 相关案例

案例一：基于 DLT 的新型供应链金融与中小微企业融资

特征对比 / 项目	传统融资模式	常规供应链金融融资
贷款对象	资质较好的大中型企业	供应链上下游企业,主要以小微企业为主
授信主体	单一企业	供应链参与主体
授信根据	企业静态信息、抵押物情况	供应链动态信息、应收账款
融资途径	传统商业银行	商业银行、保理、融资租赁等机构
风险来源	企业自有信用风险	核心企业存在的道德风险
银企关系	债权债务关系	合作共赢关系
银行风险	风险等级较小	风险等级较小
还款渠道	企业自有资产抵押	核心企业应付款及销售收入
意义作用	解决企业融资	解决小微企业融资问题,提升供应链运行效率
融资速率	较慢	较快
融资规模	融资金额一般较大	融资金额一般较小

背景：

传统供应链金融中，中小微公司获取银行授信放贷主要依赖于核心公司的担保或数据支持。然而，核心企业常利用优势地位转移成本或隐瞒数据，导致中小微企业处于劣势，同时增加银行审验成本，进而抬高中小微企业融资代价。

解决方案：

基于区块链的 DLT（分布式记账技术）与供应链金融重新“链化”成新型供应链金融

依据：

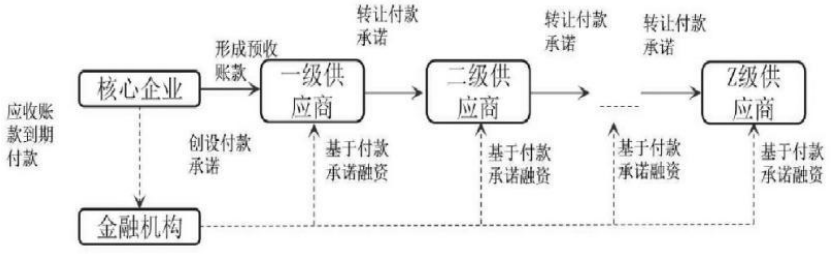
①DLT 的免中心化特性能够增强中小微公司的议价能力，分散风险，提升整个供应链金融领域的价值。所有节点处于相等位置，共同参与数据记录和处理，确保系统稳定运行。

②DLT 的透明与可追溯性、不可篡改的特点，使供应链行业更加开放透明。它能解决交易背景真实性问题，确保信息的第一手、确实和有用。每笔交易节点信息由整个网络认证，物流信息动态反映货物变化，及时通知相关方，提高行业信息透明度。

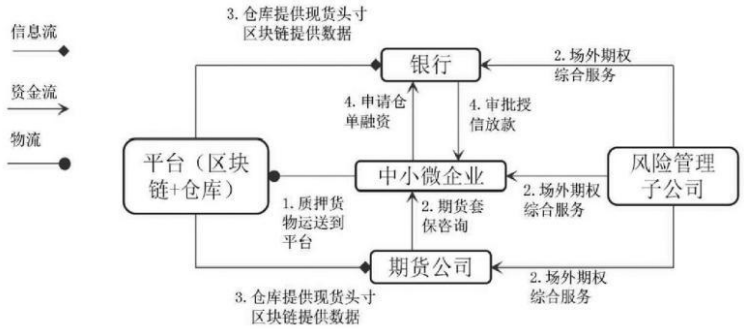
③DLT 的共识性和智能契约能降低中小微企业融资成本。在供应链融资交易中，DLT 技术减少人工介入，实现数字化管理，各参与方可共享数据，提高工作效率，降低错误率。这降低了银行贷后管理成本，从而使中小微公司贷款成本下降。

方案呈现：

第一种：信用多级传递供应链金融模式



第二种：区块链+期货供应链金融模式



案例二：Corda

https://www.oschina.net/news/94256/r3-corda-based-on-jvm-development

Corda 是一个分布式账本平台，专为金融行业设计，支持智能合约和隐私保护，常用于银行和保险领域。它被用于记录，管理和自动化业务合作伙伴之间的法律协议。它针对分散式应用程序面临的隐私和可扩展性挑战提供了独特的响应。

特点：

用 Java 和其他 JVM 语言编写的智能合约；流程框架来管理参与者之间的沟通和协商；点对点网络节点；“公证”基础设施来验证交易的唯一性和排序；启用称为 CorDapps 的分布式应用程序的开发和部署；用 Kotlin 编写，基于 JVM

技术揭秘：

（1）Corda 使用 Kotlin 作为开发语言，合约可以使用 Java、Kotlin 或者其他基于 JVM 的语言来编写。

选择 Kotlin 的原因是：相比其他目前区块链流行的语言，比如 C++ 或 Golang，Java 系有最强大的生态支持，和成熟的基础设施积累。因为是面向金融行业，应用技术栈也以 Java 为主（因为主导企业 IBM、Oracle 等为主），进而使得 adoption cost 尽可能小，开发更容易。对于金融行业这样有着厚重历史积累（技术包袱），以及各种异构系统，Java（JVM）平台有更成熟和强大的集成能力（比如数据仓库、离线计算等）。

除此之外，相比 Java 以及 JVM 平台的其他语言（Clojure、Scala、Ceylon 等），Kotlin 又平衡了语言灵活性和健壮性（相比 Java 提供了更多语言层面的改进，比 Clojure、Scala 又具备更平滑的学习曲线，同时 IntelliJ 官方对 Kotlin 的支持更强大）。

（2）共识（共识粒度小，共识范围小）

相比 BTC 或 Ethereum 这样的 Permissionless 网络，Corda 提供一个更可信任的 Permissioned P2P 网络，所有 transaction 参与者都是 authenticated 和 authorized。 所以 Corda 的共识机制舍弃了 BTC 或 Ethereum 这样的账本范围的全局共识，只要求 transaction 的所有参与者对于 transaction 达成共识。因为舍弃了对账本的全网广播，舍弃了所有节点都需要验证所有的 transaction，进而极大得提高了 transaction 的吞吐。不像 Ethereum 的基于 account 的状态机模型，Corda 采用了和 BTC 类似的基于 transaction 的 UTXO 模型，逻辑上完全对应金融系统的复式记账。

（3）Notary

Corda 中引入了 Notary 的概念，Notary 负责确保 UTXO 模型中的“输入”的有效性，比如防止 “double-spent” 攻击。它是所有 transaction 验证和确认（verify 和 validate）的基础，本质上可以认为是 Corda 这个 “半信任网络” 中的 “可信任中介”。逻辑上看是 “中心化的角色”，但实际上 Notary 可以是一个网络，甚至可以是另一个基于某种共识的公链。

（4）Command

因为面向金融行业，Corda 最重要的设计目标是支撑现实世界的各种金融活动（交易行为），所以 Corda 从 transaction 的设计，到智能合约以及 Flow 的能力，都是为了描述自然世界的交易行为和动作，比如转账、存入、提现、开票、兑付等。 所以 Corda 在 transaction 中设计了 command 这个概念，command 由 transaction 参与方来约定（含义），同时通过强制包含所有参与方的公钥来做验证（验证签名）。为了映射自然世界中各种复杂的多方交易，Corda 中引入了 “复合公钥”（composite-keys）。其中的公钥以树结构组织：所有的叶子节点就是各个参与方的 key，上层节点则约定阈值。

（5）合约

Corda 中另一核心特点就是它的合约系统，相比跑在 EVM 上的 Ethereum 的智能合约，Corda 的合约本质上就是一个实现了 Contract interface 的 Java class。这个接口只有一个用于验证 transaction 的方法 verify 和一个 annotation。

（6）Flow

Flow 是 Corda 中另一个重要的特性，本质上来说 Flow 就是一系列复杂的 Command 指令的编排，用来描述自然世界里涉及多方、多环节、有条件的复杂交易流程。因为 Corda 的共识是 transaction 级别参与方范围的，同时 transaction 的通信都是点对点的，所以 flow 的设计和实现非常直观和简单。因为面向金融行业，Corda 内置了大量开箱即用的 Flow template（在 net.corda.flows 包），基本涵盖了金融领域主要交易流程。同时 Flow 支持组合和继承，方便自定义和编排。Flow 的底层实现是基于 Quasar 的，是 JVM 平台上实现了 actor 模型的纤程 / 轻线程库（Akka 也是，但主要面向 Scala）。通过 Quasar 的 bytecode 注入，可以实现 flow 的挂起、恢复等调度，这能进一步提高 Corda 系统的伸缩能力和并发能力。

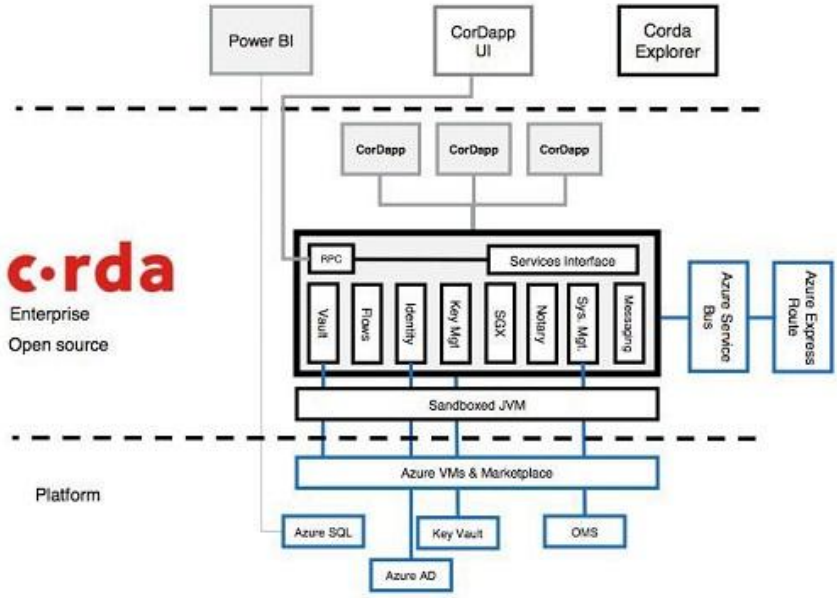
（7）数据存储

Corda 的数据存储支持标准 JPA 规范，可以通过多种 ORM 库将数据持久化到关系型数据库。目前 Corda 实现里是内置了一个 H2 数据库。由于标准的 JPA 规范，这使得 Corda 节点可以非常容易得集成 / 复用金融行业使用广泛（几乎是唯一）的企业级 RDB 系统，比如 DB2 或 OracleDB。数据层面这种开放架构，使得企业客户完全能够将 Corda 的数据和自身业务数据无缝集成。比如通过 SQL Join 来统一查询，或输入到 Hadoop 进行离线计算等。

（8）CorDapp

类似 Hyperledger Fabric，Corda 也采用了 plugin 机制来支持 CorDapp。每个 CorDapp 需要扩展 CordaPluginRegistry 这个接口来注册自己，并通过 REST API 来向外提供服务。 CorDapp 中的逻辑是通过声明或使用 flow 来实现的，客观上提高了安全性。CorDapp 会打包成 Fatjar 的形式，上传并部署到 Corda 节点的 JVM 中。

（9）Corda 逻辑架构图



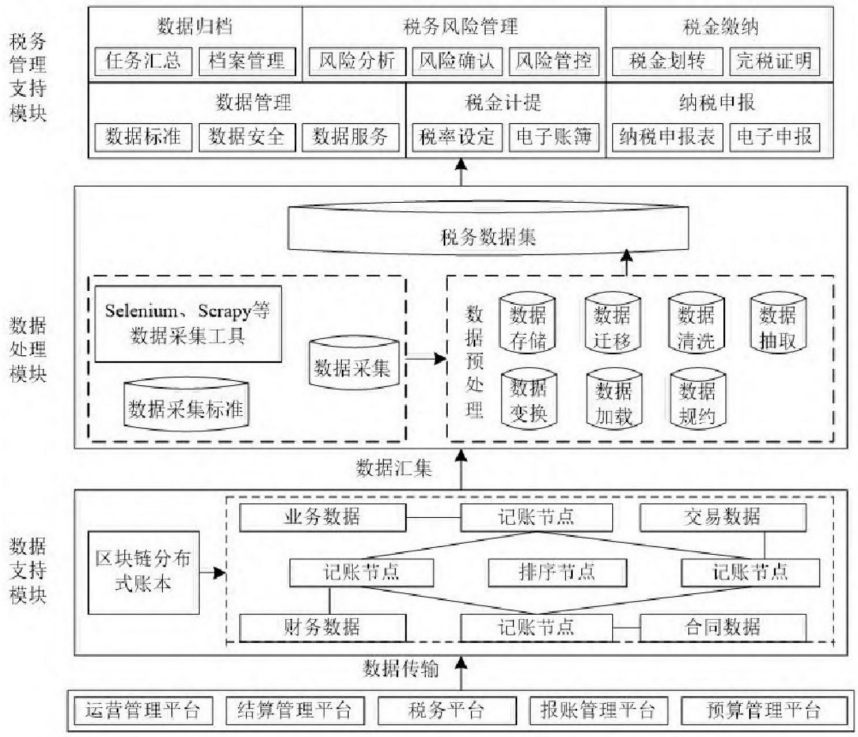
总结：

本质上，Corda 并不是去创建新的区块链（公链），而是致力于提供专门服务于泛金融行业 “去中心化的 ledger（数据库）”。

相比其他区块链系统，由于针对金融行业的定位，做了一些方面的取舍和改进：（在 Permissioned 网络环境下）降低了共识的范围和级别；缩小了数据可见性；（所以间接）具备较高的吞吐；（强化了特定合约描述能力）提供了与自然世界法律、金融的映射。加上 JVM 强大生态、完善成熟的基础设施、大量开箱即用的工具，以及内置对金融行业领域的支持。

Corda 通过“状态对象”模型确保交易隐私，仅相关方可见，适合金融行业的高隐私需求。但其生态系统相对较小，开发者资源有限。

案例三：基于 DLT 区块链的企业全周期智能税务管理研究



锐科激光充分利用现代信息技术推动税务管理工作优化升级，及时利用区块链分布式账本构建全周期智能税务管理体系，并自 2022 年起将其应用于具体税务管控活动之中，助力企业健康发展。其应用涵盖基于涉税数据管理模块，全面管理生产经营全流程税务信息；基于税金计提模块，智能精准计算企业税额数据；基于纳税申报模块，一键生成申报资料并实施智能纳税申报；基于税金缴纳模块，自动划转税金并获取完税证明等

案例四：基于 DLT 的影子银行风险监测与管理机制研究

例如安信信托的发展，当影子银行快速发展时，如果缺乏良好的风险控制能力，不仅会导致自身风险，还会出现风险溢出的问题。监管机构与金融机构、技术公司和行业协会等各方合作，共同建立了一个基于分布式账本技术的影子银行风险监测与管理平台。平台采用了加密算法、智能合约和共识机制等技术手段，确保数据的安全性、透明性和一致性。各参与方按照事先确定的权限和责任，共享和上传影子银行交易数据，并通过智能合约自动验证和记录交易信息。

案例五：区块链技术在企业供应链管理中的应用路径及效果研究

蒙牛乳业利用分布式账本技术所具备的数据共享、去中心化与模块化特性，在保证产品安全的同时让供应链的各环节信息更加透明。在销售环节，蒙牛乳业利用分布式账本技术全程留痕、可溯源的特性，将其所有销售渠道的业务流程及后续产品的交易路径记录在区块链中。同时分布式账本技术在企业供应链管理中的应用

案例六：中国人民银行数字货币电子支付（DCEP）项目

中国人民银行（PBOC）推出的数字货币电子支付项目（DC/EP）代表了全球中央银行数字货币（CBDC）的一个重要实践。DLT（在此项目中发挥了关键作用，

其不仅为数字货币提供了安全、透明的交易记录，还促进了交易的快速确认和高效清算。

1.交易记录与透明度： DLT 技术在 DC/EP 项目中用于记录每一笔数字货币的交易。由于 DLT 的分布式特性，这些交易记录是透明且不可篡改的，确保了交易的完整性和真实性。这有助于增强公众对数字货币的信任度。

2.快速确认与清算： 与传统的支付系统相比，DLT 技术允许交易在更短的时间内得到确认和清算。这降低了交易延迟，提高了支付效率。在 DC/EP 项目中，用户可以更快地完成支付，从而提高了整个支付系统的流动性和可用性。

3.安全性与隐私保护： DLT 技术通过加密手段保护用户隐私，同时确保交易的安全性。在 DC/EP 项目中，用户的身份信息被加密处理，只有授权机构才能访问敏感信息。这既保护了用户隐私，又防止了欺诈和非法交易的发生。

4.跨机构协作与标准化： DLT 技术有助于不同金融机构之间的协作和标准化。在 DC/EP 项目中，各参与机构可以通过 DLT 技术实现数据共享和交易验证，降低了跨机构交易的成本和复杂性。

案例七：监管科技

本案例探讨了区块链技术在监管科技（Regtech）领域的应用潜力，特别是针对英国抵押贷款的监管环境。监管科技作为一个相对较新的术语，旨在通过新技术减轻监管合规负担，提高风险管理效率。案例核心围绕 Maison 项目展开，该项目是一个基于 R3 的 DLT（分布式账本技术）平台的原型系统。Maison 项目的目标是解决现有监管报告程序中的一系列问题，如数据质量、处理效率和合规成本等。

DLT 技术的核心优势在于其分布式、去中心化的特性，能够实现数据的实时共享和不可篡改。在 Maison 项目中，DLT 技术被用来构建一个共享的、可信的合规数据平台。这一平台允许银行和监管机构作为节点加入区块链网络，实现点对点通信，从而提高了数据的隐私性和安全性。

通过 DLT 技术，Maison 项目解决了传统监管报告程序中的多个问题。首先，它提高了数据的质量和标准化格式，使得来自不同银行的数据能够在统一的标准下进行处理和比较。其次，DLT 技术改进了治理、透明度和责任制，在整个抵押贷款生命周期中提供了更清晰的监管视角。最后，通过 DLT 技术，规则和义务得到了更一致的解释和应用，从而降低了监管的不确定性和复杂性。

然而，DLT 技术的应用也带来了一些挑战。例如，利益相关者需要权衡效率提升与监管模式改变之间的利弊，以及考虑相关控制权的丧失问题。此外，DLT 技术的实施还需要克服技术上的障碍，如数据隐私保护、系统可扩展性和交易性能等。

案例八：比特币

比特币有一个重要的概念，就是区块链。区块链本质上是一个去中心化的数据库。比特币的底层技术是使用密码学方法相关联产生的数据块。包含这个批次网络交易的信息，自带防伪属性，用于验证是否有效，同时会生成下一个区块。

DLT（分布式账本技术）在比特币中的应用主要体现在构建和维护其底层区块链结构上。以下是 DLT 技术在比特币中的具体应用：

首先，DLT 技术为比特币提供了一个去中心化的数据库，即区块链。这个数据库由网络中的所有节点共同维护，每个节点都持有相同的交易记录副本。这种

分布式结构确保了数据的高度透明和不可篡改性。

其次，比特币利用 DLT 技术的特性，通过密码学方法将交易信息打包成数据块，并按时间顺序依次相连，形成区块链。每个数据块都包含了一定数量的交易记录，并且每个数据块都包含前一个数据块的哈希值，从而确保了数据的连贯性和一致性。

此外，DLT 技术还支持比特币网络中的共识机制，如工作量证明（PoW）。共识机制确保了分布式节点之间能够达成一致，决定了哪些交易可以被写入区块链。在比特币中，矿工通过解决复杂的数学难题来竞争记账权，成功解题的矿工将新区块添加到区块链中，并获得一定数量的比特币作为奖励。

总的来说，DLT 技术在比特币中的应用不仅为其提供了一个安全、透明、不可篡改的交易记录平台，还通过共识机制确保了网络的稳定性和安全性。这些特性使得比特币成为了一种去中心化、无需信任中介的数字货币，为金融领域带来了创新。

案例九：Defi-去中心化的金融服务

功能	服务	加密金融体系		传统金融体系
		去中心化金融（DeFi）	中心化金融（CeFi）	
交易	资金转移	去中心化稳定币（如 DAI）	中心化稳定币（如 USDT 和 USDC）	传统支付平台
	资产交易	去中心化加密货币交易所（如 Uniswap）	中心化加密货币交易所（如币安和 Coinbase）	交易所和场外经纪商
	衍生品交易	去中心化加密衍生品交易所（如 Synthetix 及 dYdX）		
借贷	担保贷款	去中心化加密借贷平台（如 Aave 和 Compound）	中心化加密借贷平台（如 BlockFi 和 Celsius）	活跃于回购和证券借贷的做市商
	无担保贷款	加密信用协议（如 Aave）	加密银行（如 Silvergate）	商业银行和其他非银行贷款
投资	投资工具	去中心化加密投资组合（如 Yearn 和 Convex）	加密基金（如 Grayscale 和 Galaxy）	投资基金

DeFi，即去中心化金融，是区块链技术在传统金融领域的一大创新。它利用智能合约实现金融服务的去中心化，颠覆了传统金融的某些服务范式。

传统金融体系大多由中心化的数据库系统组成，存在诸多中介、高额手续费和效率问题。而 DeFi 通过区块链技术，实现了金融业务的代币化，无需中心化中介即可提供金融服务。每个人都可以通过智能合约直接参与金融活动，进行点对点的交易，大大降低了交易成本，提高了效率。

DeFi 主要集中在去中心化借贷、自动化做市商、去中心化交易所、稳定币发行四大板块。其中，去中心化借贷允许用户无需传统银行即可进行借贷活动；自动化做市商则通过算法提供流动性，无需人工干预；去中心化交易所实现了用户之间的直接交易，无需中心化交易所作为中介；稳定币发行则提供了稳定的数字货币，用于去中心化金融系统中的支付和结算。

DeFi 具有开放、透明、去中心化的特点。它使用数字货币作为底层的支付手段，通过智能合约实现金融协议的执行。智能合约具有自我执行、自我监管的特点，无需法务和法官的参与。同时，因为建立在区块链上，所有交易都可以被追溯，保证了透明性和公平性。

此外，DeFi 天生无国界且去中介，为全世界没有银行账户的人提供了金融服务的机会。它只需要一个钱包即可参与金融活动，大大降低了传统金融服务的门槛。

Defi（去中心化金融）的主要项目包括 Uniswap 和 Compound。

1.Uniswap 是基于以太坊的去中心化代币交换协议，解决了传统交易所中心化的问题。它是一组部署在以太坊上的智能合约，用户可以在链上自由进行代币兑换，无需注册、身份验证或提取限制。相比其他 DEX，Uniswap 的 gas 利用率高，费用更便宜，且交易对手是代币池，采用自动做市模型计算价格。Uniswap 的公开智能合约保证了交易的透明和真实，体现了去中心化金融的包容、创新和公平。

2.Compound 则是一个允许用户借贷代币的智能合约，类似于银行但利息复利计算且比传统银行高。借贷者通过超额担保在 Compound 中借款，如果借款能力低于 0，抵押品将被出售偿还债务。贷款利率根据资产需求决定，每个 ERC-20 代币在 Compound 中都有自己的借贷市场。用户只需选择借款币种，无需沟通还款日期、利率等即可借款，实现了实时且可预测的借款过程。Compound 作为去中心化银行，利润分配更公平合理，智能合约保障了违约行为的杜绝，避免了金融风险。

然而，分布式数据库在金融级应用场景中仍面临挑战，如何在确保数据一致性的前提下，同时保障系统的高性能和高可扩展性，是分布式数据库的核心技术难题。这需要在保证数据准确性的同时，不断优化系统架构和技术，以满足金融领域对高性能和高可扩展性的需求。

参考文献:

[1] 王嘉瑶,王婷,袁文亮,等.分布式账本技术的发展历程研究综述[J].计算机应用研究,2023,40(03):641-648.10.19734/j.issn.1001-3695.2022.07.0394.
[2] 袁敏.基于区块链分布式账本的企业全周期智能税务管理研究[J].财会通讯,2025(02):150-154.10.16144/j.cnki.issn1002-8072.2025.02.029.
[3] 牟婷钰.基于分布式账本技术的影子银行风险监测与管理机制研究[J].现代商业,2024(13):145-148.10.14097/j.cnki.5392/2024.13.039.
[4] 颉茂华,张家春,王艺茹,等.区块链技术在企业供应链管理中的应用路径及效果研究——以蒙牛乳业为例[J].管理案例研究与评论,2024,17(02):280-296.
[5] 《主流企业区块链的技术分析：以太坊，Fabric，Corda》 https://zhuanlan.zhihu.com/p/270586016
[6] 【案例研究 | 区块链在监管科技中的应用 - CSDN App】

https://blog.csdn.net/BitTribeLab/article/details/107711779?sharetype=blogdetail&shareId=107711779&sharerefer=APP&sharesource=2401_84383193&sharefrom=link