

区块链概念简介

了解区块链协议如何实现信任。学习如何评估在方案中使用区块链的时机并确定区块链是否适合自身解决方案。

学习目标

在本模块中，你将了解如何：

- 说明区块链如何实现参与者之间的信任和业务流程。
- 评估在解决方案中使用区块链的时机。

先决条件

- 编程概念的基本知识，例如变量和条件逻辑

简介

实施涉及多个公司的解决方案可能会非常困难，因为需要信任合作伙伴的数据。大多数情况下，你会使用集中式数据库。数据存储在一个作为可信源的位置。维护数据库的公司必须是受信任的中央数据机构。

要在不使用中央数据库的情况下信任数据和参与者，可以使用区块链来实现业务流程。

假设你是解决方案架构师，供职于一家生产冰淇淋的乳制品加工公司。你通过供应链接收来自多个牛奶场的未加工牛奶。你的公司将包装好的冰淇淋运输至多个零售商。运输过程中温度不正确，导致产生食物质量和安全问题。因为有多个公司负责运输和存储产品，因此很难识别供应链中出错的一方。你需要创建一个系统，用于快速识别供应链中的问题。每个供应链公司都想要将其现有系统与该解决方案集成，并在出现食物安全召回事件时自主审核运输情况。



本模块介绍区块链如何让业务合作伙伴在没有中央机构的情况下信任彼此的数据。还简要介绍了区块链的工作原理。目标是帮助你确定区块链是否适合自身方案。

学习目标

在本模块中，你将了解如何：

- 说明区块链如何实现参与者之间的信任和业务流程。
- 评估在解决方案中使用区块链的时机。

先决条件

- 基本了解编程概念，例如变量和条件逻辑。

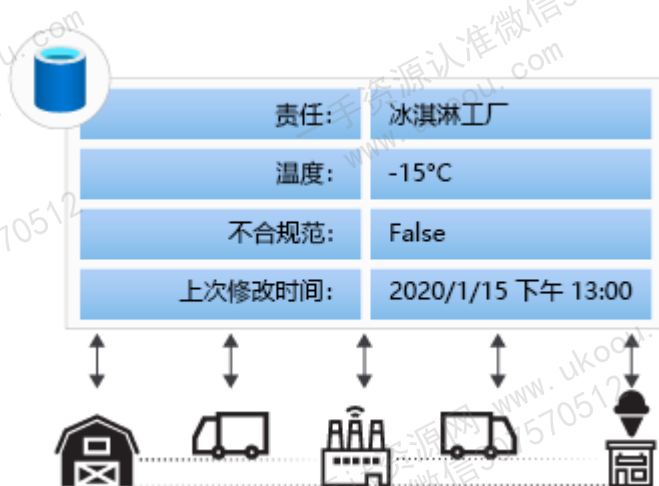
什么是区块链？

区块链是一种用于保留记录和执行合同的技术，它通过使用加密来确保难以更改以前的历史记录。它允许参与者通过跟踪共享账本的更改来共享工作流程。

在冰淇淋方案中，我们如何发现由于运输过程中存储温度不当导致的食物质量或安全问题？我们需要跟踪责任方和温度，并记录更改。

为什么不使用集中式数据库？

我们可以建立一个集中式数据库，让所有参与者使用它来跟踪运输。在许多方案中，集中式数据库都是适当的解决方案。假设我们有一个集中式数据库，该数据库存储有关元素和当前责任方的详细信息。在我们的方案中，我们可以让农场主、承运方、工厂和零售商使用同一个集中式数据库。

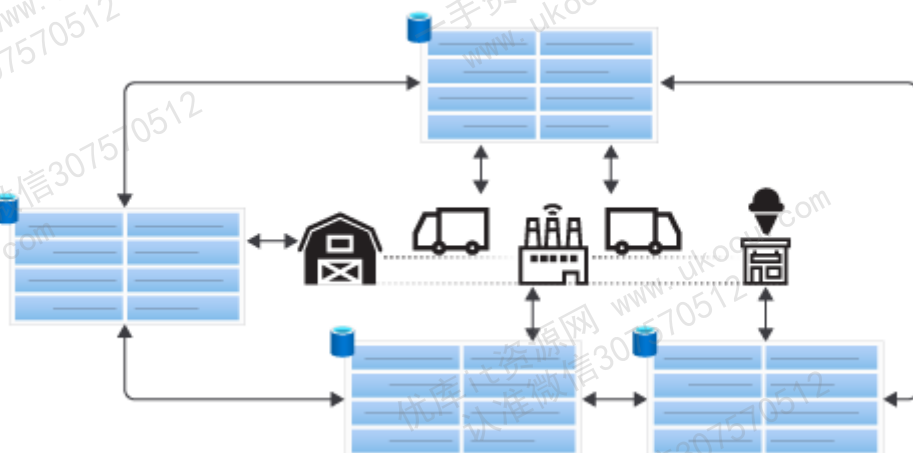


集中式数据库的优点是可以轻松控制访问权限和一致性。每一方都使用相同的数据库，并由受信任的机构控制访问权限。由于只有一个数据库，因此所有参与者都使用相同的数据集。所有参与者都需要相信数据库是准确的，引申一下，就是他们需要信任数据库的所有者不会出于任何目的修改历史数据。

如果我们的方案不允许存在受信任的中央机构，该怎么办？如果没有一家公司愿意负责托管集中式数据库，该怎么办？可能无法满足与每个参与者的系统集成要求。

分布式数据库

如果每个参与者都有数据库的副本，会怎样？分布式数据库使用数据库的多个副本，并同步更改。在我们的方案中，可以让农场主、承运方、工厂和零售商使用自己的分布式数据库。

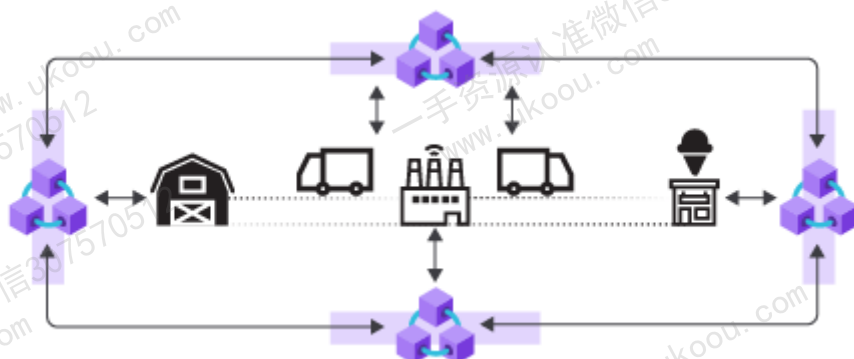


分布式数据库的优点是每个参与者都有数据库的副本。在自己的数据库副本中，通常能更轻松地控制访问权限以及集成系统和流程。但是，需要同步每个数据库的更改。处理失败和冲突可能会增加复杂性和数据诚信问题。

分布式账本

区块链技术称为分布式账本。与会计账本一样，分布式账本也是事务的历史记录。账本中的每个事务都会影响最终状态。

分布在参与者之间的区块链网络称为联盟网络。通过联盟网络，每个合作伙伴都能查看网络中发生的每个事务。



区块链使用共识规则确保不同节点之间数据的一致性。它还使用加密技术，让参与者能信任数据。具体而言，它会阻止任何一个参与者或少数参与者修改历史记录。区块链是分散的，因此最适合可以使用分散式数据库的解决方案。例如，由于成本、控制或成为单一故障点方面的原因，你需要在没有中央机构的情况下支持多个公司。

区块链的工作原理

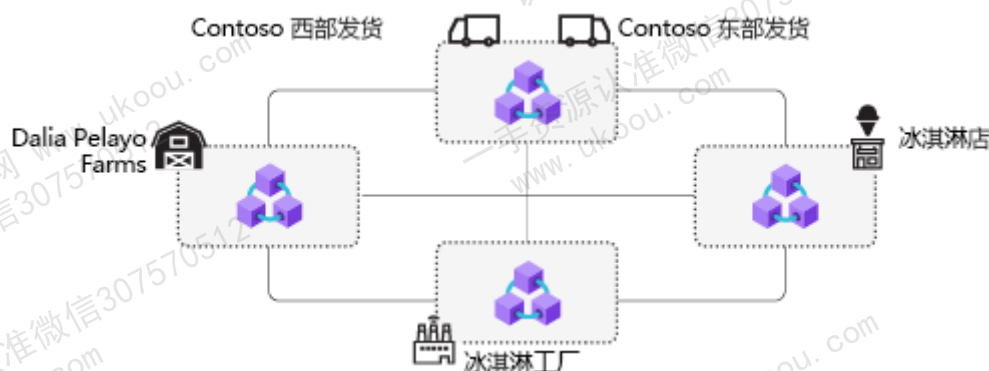
现在我们已了解区块链的基础知识，接下来我们来看看它的工作原理。这些信息可帮助你确定区块链是否适合自身方案。

数据是如何分布的？

在我们的方案中，假设有多家公司。我们在乳制品加工公司建立了一个集中式数据库。但所有参与者都不想成为中央机构。我们可以使用区块链分布式账本。使用区块链将不再需要中央机构。此外，拥有区块链节点的每个参与者都可获得账本副本，以便他们能够自行审核并与自己的系统集成。但并不要求每家公司都设置自己的下级节点。合作伙伴之间可以共享这些节点。

每个节点都通过区块链网络连接到其他节点。例如，Dalia Pelayo 农场、冰淇淋工厂和冰淇淋店都各自管理着一个节点。Contoso West 和 Contoso East 是同属一家母公司的两个独立合作伙伴。

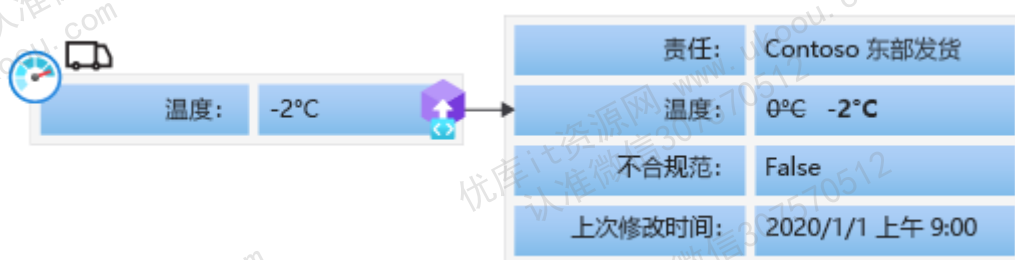
Contoso 有一个节点。节点与公司之间不必存在一对一关系。



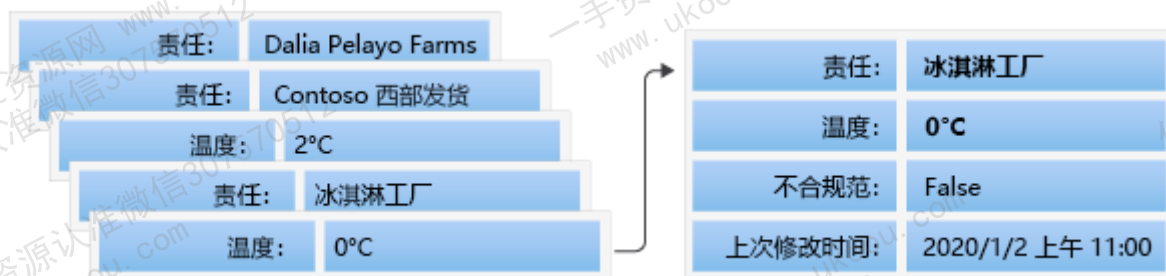
更改状态

区块链中的数据表示状态。这就是为什么区块链非常适合使用加密货币之类的数字令牌。我们可以把这种情况想象为实际货币的所有权：一枚硬币一次只能在一个人的口袋。如果硬币在你的口袋，所有权就是你的。如果将硬币给朋友，状态就会变为你的朋友拥有这枚硬币。在我们的方案中，货物运输通过供应链。产品的责任方也随运输转移。我们想知道的数据包括责任方、温度以及产品是否合规。

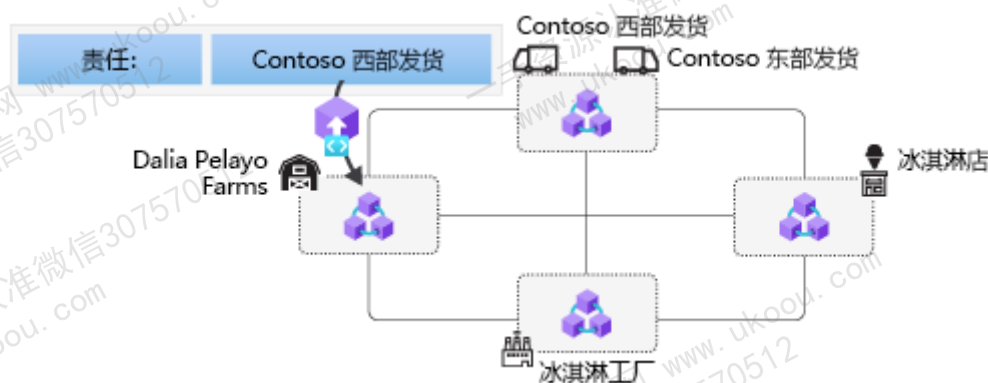
区块链使用事务将数据的状态从一个值更改为另一个值。例如，如果我们需要知道冰淇淋是否在低于冰点的温度下存储。在运输冰淇淋的过程中，温度传感器会定期报告温度。报告的温度是一个事务，会发送到区块链事务节点。



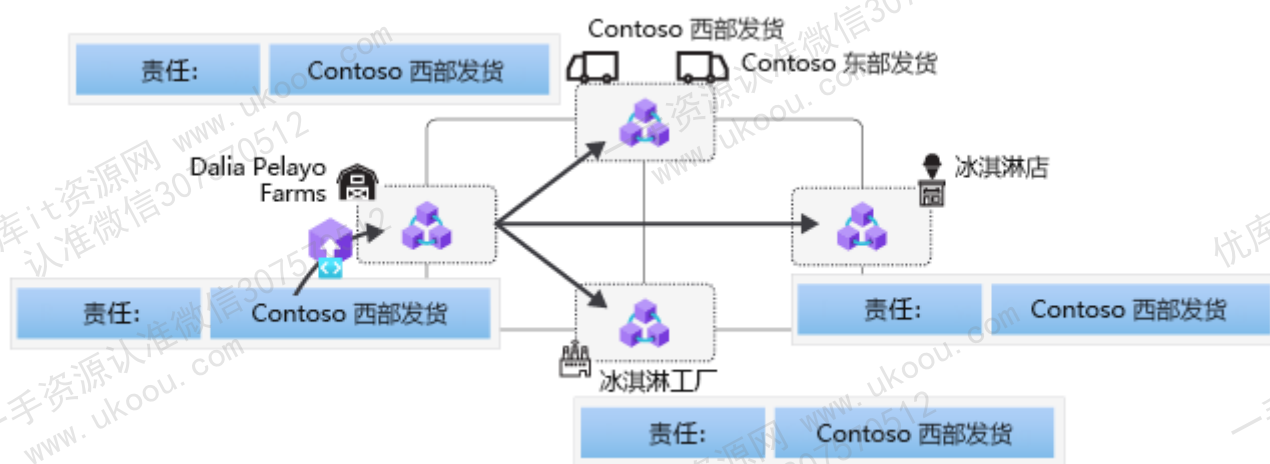
在冰淇淋方案中，在货物运输通过供应链的过程中，每当状态发生更改时，都会发送一个事务。例如，下图展示了向冰淇淋工厂运送货物的典型事务。每个事务都更改了责任方或温度。账本的当前状态是按顺序应用的事务。



发送事务时，会发送到区块链事务节点。假设 Dalia Pelayo 农场通过 Contoso West Shipping 运输牛奶。Dalia Pelayo 农场的发货系统会向自己的区块链节点发送一个事务。该事务会将运输责任方从农场主更新为 Contoso West Shipping。



在整个区块链网络中，区块链都会发送事务。每个节点都会获取事务的副本。



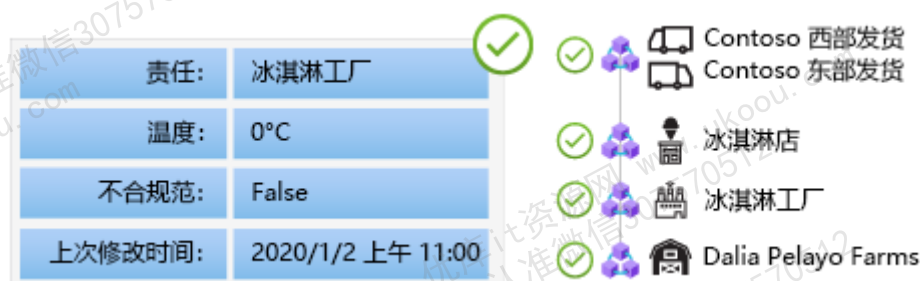
每个节点都会处理事务，但仍需要使用共识机制进行验证。共识实现了分布式账本的一致性和信任。

如何确保账本数据的一致性？

在分布式网络中，很难确定什么是真实的，因为所有节点都存在数据更改。如果冰淇淋工厂节点没有收到运输事务，会发生什么情况？他们如何知道牛奶已从农场运出？如果运输公司的冷藏车出了故障，牛奶变质了怎么办？送货公司是否会通过修改账本来逃避责任？

区块链采用一种共识机制，可验证所有区块链节点上的数据并达成一致。共识提供一种方法，让所有分散管理的节点都达到相同的状态。在转移价值或责任时，顺序很重要。例如，如果你将汽车的所有权转给朋友，就无法再将该项所有权转给同事。此类问题称为双重花费，可通过共识机制解决。共识

可确保事务的顺序正确以及区块链的诚信。共识的原理是，一组事务作为一个块进行验证，至于这个块是否应属于区块链，整个网络必须达成一致。



有几种区块链共识算法，包括工作证明、所有权证明和授权证明。每个算法都以不同的方式解决一致性问题。简而言之，共识提供了一种方法，让分布式账本能达成共同的状态。

什么是块？

块是区块链中存储事务信息的数据群集。块中的事务数通常是基于时间的。例如，下图显示的块包含了过去 10 分钟内发生的事务。



经过共识后，已验证的块会添加到每个节点的区块链中。由于所有节点在该链中都具有相同的块，所以账本能在网络上保持一致。因此，所有节点都以一致的顺序包含相同的已验证数据。

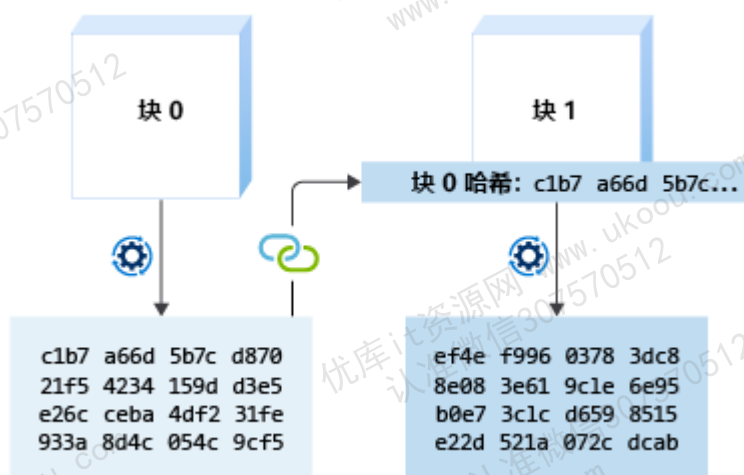
如何确保账本不可变？

你可能会认为，如果能控制自己节点中的账本，就能更改副本中的数据。这些数据怎么会不可变呢？

区块链使用加密哈希在块之间创建链接。将块链接在一起后，可以通过共识算法确定事务顺序的一致性。加密哈希是一种算法，可将任意大小的数据映射到固定大小的位表示形式。我们可以将其视为数字指纹。比特币使用 SHA-256 哈希算法。如果在 100 页的文档上使用 SHA-256 哈希函数，则函数输出是一个 256 位哈希值。如果只更改文档中的一个字符并重新生成了哈希，则输出是一个不同的 256 位哈希值。现在，假设我们将一个块用作哈希函数的输入。输出是块中数据的唯一哈希值。



区块链使用哈希来检测这些块有没有发生任何更改。通过在生成下一个块的哈希时包含上一个块的哈希值，这些块会通过哈希链接在一起。



区块链通过使用哈希来证明数据历史记录未更改，从而实现信任。通过在创建新块时包含上一个块的哈希，将按顺序创建不可变的事务链。



如果修改链中的任何块，后面块的哈希将有所不同。验证时就会发现差异。

受信任的逻辑




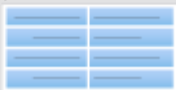
通过区块链，我们可以存储一致且可信的数据。如何添加在每个节点一致执行的逻辑？

在我们的方案中，需要使用逻辑来将产品的责任从一个参与者转到另一个参与者。我们还需要使用 IoT 温度传感器中的数据来了解温度是否过高。

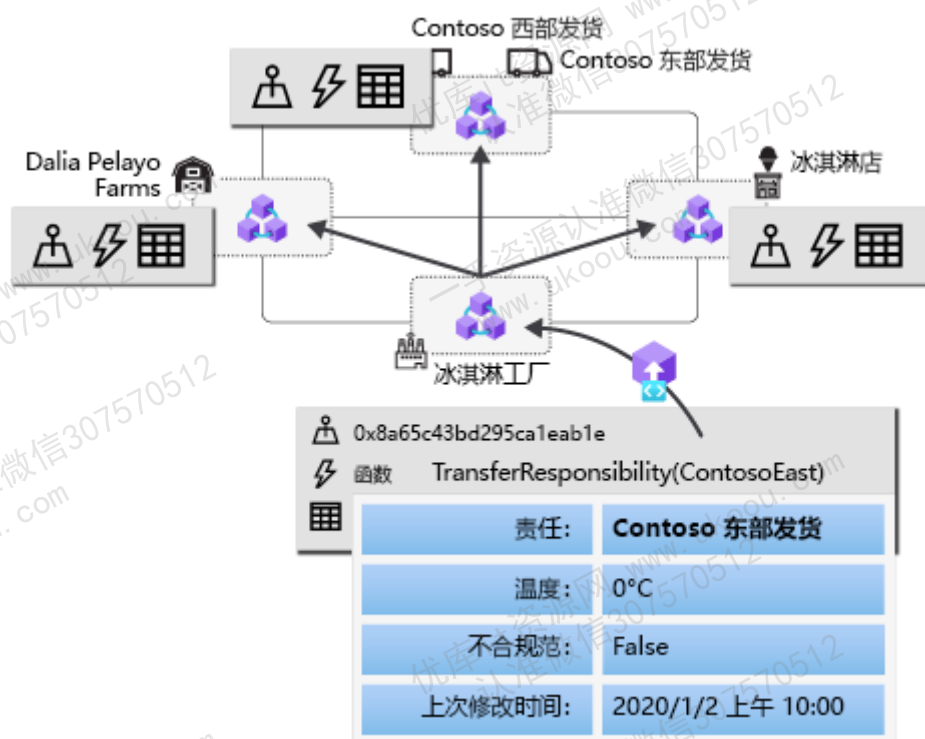
分散式应用程序 (DApp) 是分布式计算系统上的应用程序。在本模块中，我们重点介绍如何使用 Ethereum 区块链协议。Ethereum DApps 称为智能合同。智能合同包含作为事务的一部分执行的逻辑。

辑。在 Ethereum 上，我们使用名为 Solidity 的编程语言对逻辑进行编程。

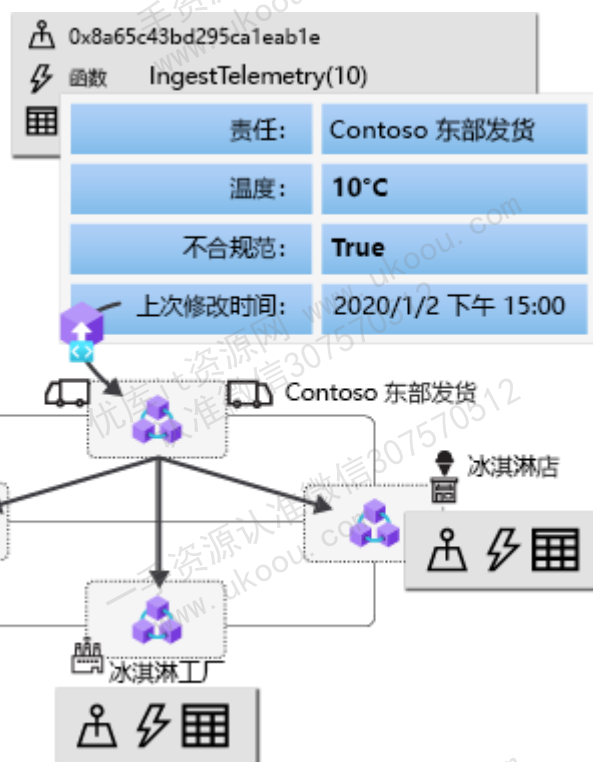
智能合约部署到区块链，并按地址引用。要使用智能合约，需创建一个实例。智能合约实例包含状态数据和程序逻辑。在我们的方案中，智能合约实例包含各种数据，例如负责的参与者、位置以及产品温度是否不合规等。我们可以执行函数来转移责任或接收实例的温度遥测数据。

地址 	0x8a65c43bd295ca1eab1e
逻辑 	function TransferResponsibility(address newCounterparty) function IngestTelemetry(int temperature, int timestamp) public
数据 	

将产品的责任转到另一方时，会执行事务。智能合约逻辑会更新状态数据。在我们的冰淇淋方案中，冰淇淋工厂运输系统会为新的冰淇淋运输活动创建一个智能合约实例。工厂运输系统将发送一个事务，该事务调用 TransferResponsibility 函数以将运输责任方改为 Contoso East shipping。区块链网络将该事务发送到所有节点。每个节点都会执行该智能合约逻辑。



在运输过程中，如果制冷装置出现故障且冰淇淋温度升至冰点以上，会怎样？IoT 温度传感器会监视冰淇淋温度并定期发送事务。如果温度高于冰点，智能合约逻辑会将这批货物标记为不合规。



由于事务包含在块链中，因此当货物状态变为不合规时，会有一个不可变的记录。冰淇淋店可以拒绝收货，避免产生食物安全问题。

与区块链中的数据一样，智能合同也是不可变的。逻辑在部署后便不能更改。因此，你可以信任智能合同逻辑始终在所有节点上一致地执行。任何代码更改都需要在新的地址部署新的智能合同。

区块链类型

区块链可以是公共的或专用的。这两种不同的类型决定了谁能参与区块链网络。

公共

如果你需要不信任任何人的网络，会怎样？任何能访问 Internet 的人都可加入你的区块链网络。不需要进行登录，也不需要向机构申请权限。

公共区块链分散在网络上，且不存在中央机构。网络上的任何节点都可以看到区块链中的所有事务。

第一个区块链网络为比特币创建。比特币区块链网络是公共的。任何人都可以查看所有事务。例如，可以使用[块资源管理器](#)查看最新的比特币块和事务。

公共区块链的共识算法使用加密货币作为验证块的奖励。公共区块链在验证事务时还可能收取加密货币费用。公共区块链的隐私保护有限。如果想要保持事务的私密性，应仅与事务中的其他参与者共享公钥。

专用

如果我们部分信任区块链网络的参与者，会怎样？只有受邀加入区块链网络的参与者才能访问区块链中存储的信息。专用网络是不完全受信任的网络。在专用网络中，所有参与者就区块链的利用方式达成了协议。

联盟区块链是专用区块链，但权限是分布式的，并按网络的最大利益行事。

在我们的方案中，我们想保持事务的私密性。联盟区块链可以限制谁有权参与共识。通过限制为只有参与者可以加入验证来实现信任。由参与者构成的组称为联盟。联盟区块链的共识算法可以使用权限而不是加密货币。

我们可能还需要保持部分数据的私密性。例如，各方都知道产品已运出，但可以保持运输细节的私密性。由于我们使用多家运输公司，双方之间的运输细节可能会保密。相互竞争的运输公司只会知道事务发生了，无法查看运输细节。

区块链协议

有几个区块链协议。最有名的是比特币。比特币区块链网络专为比特币加密货币创建。比特币区块链网络的主要功能是存储比特币值。这些值可以通过不可信的方式从一处转到另一处。

Ethereum 是通用协议。Ethereum 扩展了比特币创建的内容，提供允许编写小型程序而不仅仅是进行简单价值转移的协议。最终效果是能添加逻辑和代码，而不是进行简单的固定值转移。

如果要将区块链用于自己的解决方案，请考虑使用 Ethereum 和 Hyperledger Fabric 之类的通用协议。它们是可用于多个方案的可编程区块链。通用协议使用智能合同对业务逻辑和状态进行编码。在本模块中，我们将重点介绍 Ethereum 协议。

区块链的使用时机

区块链技术最适用于某些方案。不应将其用作常规用途解决方案。在许多情况下，集中式数据库是一个更好的选择。考虑使用区块链时，请思考几个关于自身方案的问题。

参与者

- 是否需要支持多个合作伙伴或公司？
- 是否要避免存在中央机构？也许对任何一个参与者都不信任。参与者可能不想依赖于第三方。
- 参与者是否共享数据或使用涉及多个或全部参与者的工作流？区块链技术能保证所有节点的一致性。大多数其他企业对企业 (B2B) 解决方案依赖于同步。同步数据会使 B2B 系统产生断裂和费用。分布式数据的一致性 is 区块链技术的关键优势。

性能

- 事务吞吐量是否较低？根据区块链协议和共识机制，事务处理速率可能较低。
- 与其他业务合作伙伴进行交互时，是否定义了业务逻辑？在事务中执行业务逻辑可能会影响性能。

业务逻辑

- 业务逻辑是否简单？在公共区块链上执行复杂的智能合同函数比简单的函数需要更多的加密货币。

- 业务逻辑是否是静态的且不会更改？区块链数据不可变，要更改智能合约逻辑，就需要将新合同部署到新地址。请考虑如何控制业务逻辑的版本。

信任

- 参与者之间是否需要信任和诚信？
- 事务的顺序是否重要？
- 事务是否具有私密性？