区块链技术基础：术语和用例

区块链的关键术语和无限可能的潜在应用场景

区块链技术是目前的一个流行主题。了解这一热门术语，看看企业如何利用此新兴技术获利。

1.区块和区块链

区块链是一种分布在整个业务网络上的共享账本。业务交易被永久记录在仅附加到账本的**区块** 中。所有经过确认和证明的交易都从创始区块一直链接到最新的区块，因而得名**区块链**。区块链是自网络中的区块链启动以来发生的所有交易的历史记录。区块链被用作该网络的单一事实来源。

区块链网络可以是许可网络或无许可网络。**无许可** 网络向所有参与方开放，参照网络上的已有规则对交易进行验证。任何参与方都可以查看账本上的交易，即使参与方是匿名的。比特币是人们最熟悉的一个无许可网络示例。

另一方面，**许可** 网络仅能由给定业务网络中的参与者访问。在许可区块链上，参与者只允许查看与他们相关的交易。Hyperledger Project 就是为支持许可区块链的开发而创立的。

2.交易、资产和一致性

交易 是传输到账本或从账本传出的资产。任何可被拥有或控制来产生价值的事物都是**资产**。资产可以是有形的（比如住宅或汽车）或无形的（比如抵押或租赁）。

> **深入了解区块链网络概念**
>
> 在 “分布式账本简介” 中了解区块链网络的优势。

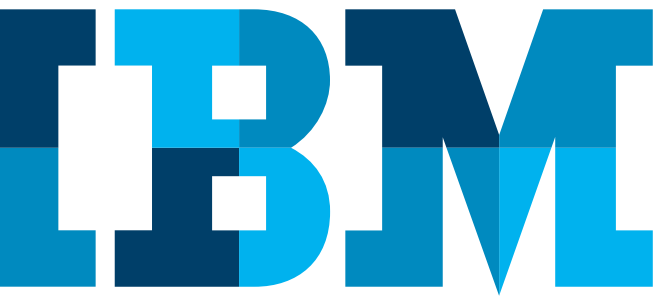
账本中的条目被同步到网络中的所有账本。区块链网络中的参与方处理的每个账本副本被称为**节点**。节点之间的**一致性**能确保共享账本是精确的副本，并降低发生交易欺诈的风险，因为篡改需要同时在许多地方进行。

要实现一致性，所有参与者都必须同意交易并通过对等网络验证它。参与者还可以建立验证交易的规则。与无许可区块链中存在的更高成本相比，受信任的参与者网络可减少在节点之间建立一致性的成本。

3.密码哈希算法和数字签名

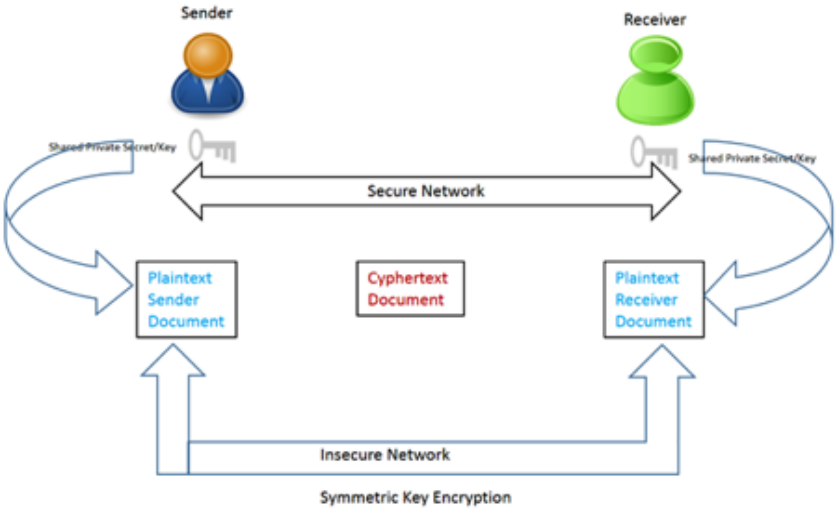
密码哈希算法（比如 SHA256 计算算法）利用可变大小的交易输入生成一个固定大小的唯一哈希值（被称为摘要）。哈希运算包含一个数学属性，那就是一个给定输入只能得到一个唯一的哈希值，但不能从哈希值推导出输入。一个给定的输入总是会计算出相同的哈希值。

对交易输入的任何修改或改动 — 甚至是最细微的更改 — 都会导致计算出不同的哈希值，这表明交易输入可能被损坏。因此，可使用哈希值检测交易输入的完整性。

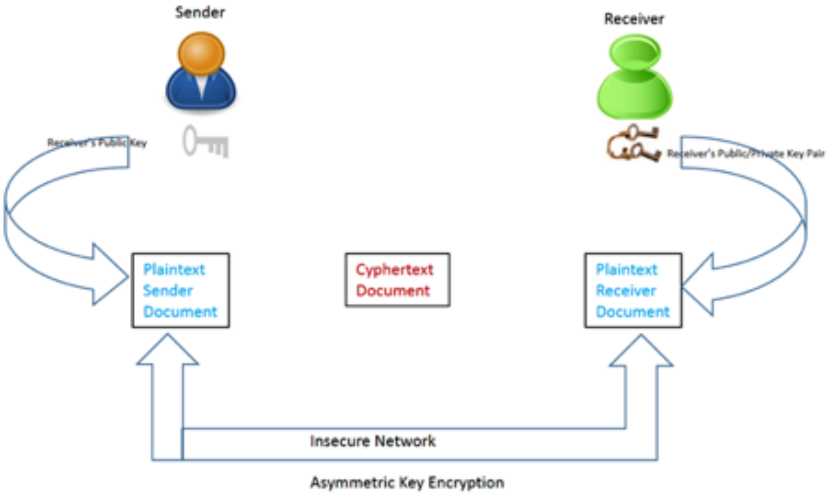


数字签名 可以确保接收者收到的交易数据中没有包含修改或伪造过的交易内容，还可以确保交易源自发送方（已使用私钥进行签名），而不是来自冒充者。

对称密钥加密使用一个私钥来加密和解密数据。该密钥必须使用一个安全网络进行共享，而数据可在不安全的网络上广播，但能由拥有该私钥的各方读取：



区块链技术使用了**公钥加密**，也称为**非对称密钥加密**。在公钥加密中，每个参与者都有一个公钥/私钥对。发送者可以使用接收者的公钥来加密数据。然后只能使用接收者的私钥读取文档或数据。非对称密钥加密在传输数据时无需使用安全网络来交换密钥。



4.智能合约和链代码

要使用拟议的交易来更新账本，每个节点必须按照**智能合约** 的逻辑来处理交易。智能合约由直接在复制的网络上运行的程序组成。智能合约使用一种编程语言在区块链上对业务规则或合同进行编码，由网络中的所有参与者执行。这些程序在 Hyperledger Fabric 中称为**链代码**，它们被复制到网络中的每个节点，并由拥有权限的各方调用来传输资产。

链代码必须是确定的，也就是说，相同的输入必须始终产生相同的输出。因此，每个节点可以相信它和对等节点处理的是同一个交易。

关于 Hyperledger Fabric

Hyperledger Fabric 是为业务用途而开发区块链应用和解决方案的基础。可以在 The Linux Foundation Hyperledger Project 中了解它的 重要概念 和 术语表。

区块链应用

一个区块链应用需要 3 个相互依赖的组件：面向用户的应用、智能合约和账本。

顶层是**面向用户的应用**，用于满足网络参与者的需求。该应用让用户调用智能合约在业务网络中触发交易。**智能合约** 封装网络的业务逻辑：资产、所有权和传输方式。每次调用智能合约，都会在网络中创建一个交易并更新账本。**账本** 持有智能合约数据的当前值（如 vehicleOwner=Daisy），并分发到整个网络。

区块链用例

区块链技术对许多行业而言是一种潜在的颠覆性技术，因为它能更顺利、更高效地组织活动。而且它能协调参与者之间更大规模的活动。下面给出了一些可从区块链技术中受益的用例：

- 物联网
  - 设备管理
- 医疗保健
  - 电子医疗记录
  - 病毒库
  - 种子库备份
  - 医生-供应商 RFP 服务和保险合同
  - 区块链健康研究共享空间
  - 区块链健康司法人员
- 金融服务
  - 信用证
  - 公司债务和债券
  - 交易平台
  - 支付汇款
  - 再购买协议
  - 外汇
- 保险
  - 索赔处理
  - P2P 保险
  - 所有权
  - 销售和承保
- 政府
  - 政府招标程序
  - 选举
  - 税收
- 工业
  - 制造流程
- 零售
  - 顾客忠诚度
- 跨行业
  - 身份管理
  - 信托行业
  - 资本资产管理
- 其他行业
  - 游戏
  - 音乐

了解更多用例

在 The Linux Foundation Hyperledger Project 上了解主要用例 的参与者和组件。

结束语

通过了解区块链中的主要术语，您可能已经开始欣赏这种重要颠覆性技术的工作原理，并且知道将它应用于哪些行业中了。

可以通过试用 IBM Bluemix 上的 Blockchain 服务，更深入地了解区块链技术。只需一次单击，就可以创建您自己的区块链网络。

如果尚未这样做，请花点时间查阅 Bluemix（IBM 的基于 Cloud Foundry 的公共云），以便了解应用程序开发和部署。试用 Blockchain 服务或 Bluemix 中的数百种云服务，开始 免费 30 天的 Bluemix 试用。或者更好的是，您是否知道 developerWorks Premium 提供了 Bluemix 的 12 个月订阅和 Bluemix 上的 240 美元云额度?进一步了解 developerWorks Premium 如何帮助您 快速开始开发适用于云的应用或将应用迁移到云。

联系IBM

了解更多 IBM Bluemix 云平台信息：https://www.ibm.com/cloud-computing/cn/zh/newplatform/

拨打 IBM Bluemix 云平台免费咨询热线（工作日 9:00-17:00）：400-065-6183

发送电子邮件至：ibmcloud@cn.ibm.com 或填写表单，IBM 业务专家会及时回复。

您还可扫描二维码关注微信公众号“IBM云计算”了解最新资讯