身份

什么是身份?

区块链网络中的不同参与者包括 Peer 节点、排序节点、客户端应用程序、管理员等。每一个参与者（网络内部或外部能够使用服务的活动元素）都具有封装在 X.509 数字证书中的数字身份。这些身份确实很重要，因为它们**确定了对资源的确切权限以及对参与者在区块链网络中拥有的信息的访问权限。**

此外，数字身份还具有 Fabric 用于确定权限的一些其他属性，并且它为身份和关联属性的并集提供了特殊名称——**主体** 。主体就像 userID 或 groupID，但更灵活一点，因为它们可以包含参与者的身份的各种属性，例如参与者的组织，组织单位，角色甚至是参与者的特定身份。当我们谈论主体时，它们是决定其权限的属性。

要使身份可以被**验证**，它必须来自**可信任的**权威机构。成员服务提供者（Membership Service Provider，MSP）是 Fabirc 中可以信任的权威机构。具体地说，一个 MSP 是定义管理该组织有效身份规则的组件。Fabric 中默认的 MSP 实现使用 X.509 证书作为身份，采用传统的公钥基础结构（Public Key Infrastructure,PKI）分层模型（稍后将详细介绍PKI）。

一个简单的场景来解释身份的使用

想象你去超市购买一些杂货。在结账时，你会看到一个标志，表明只接受 Visa，Mastercard 和 AMEX 卡。如果你尝试使用其他卡付款（我们称之为“想象卡”）无论该卡是否真实、或你的帐户中是否有足够的资金，都无关紧要。它不会被接受。

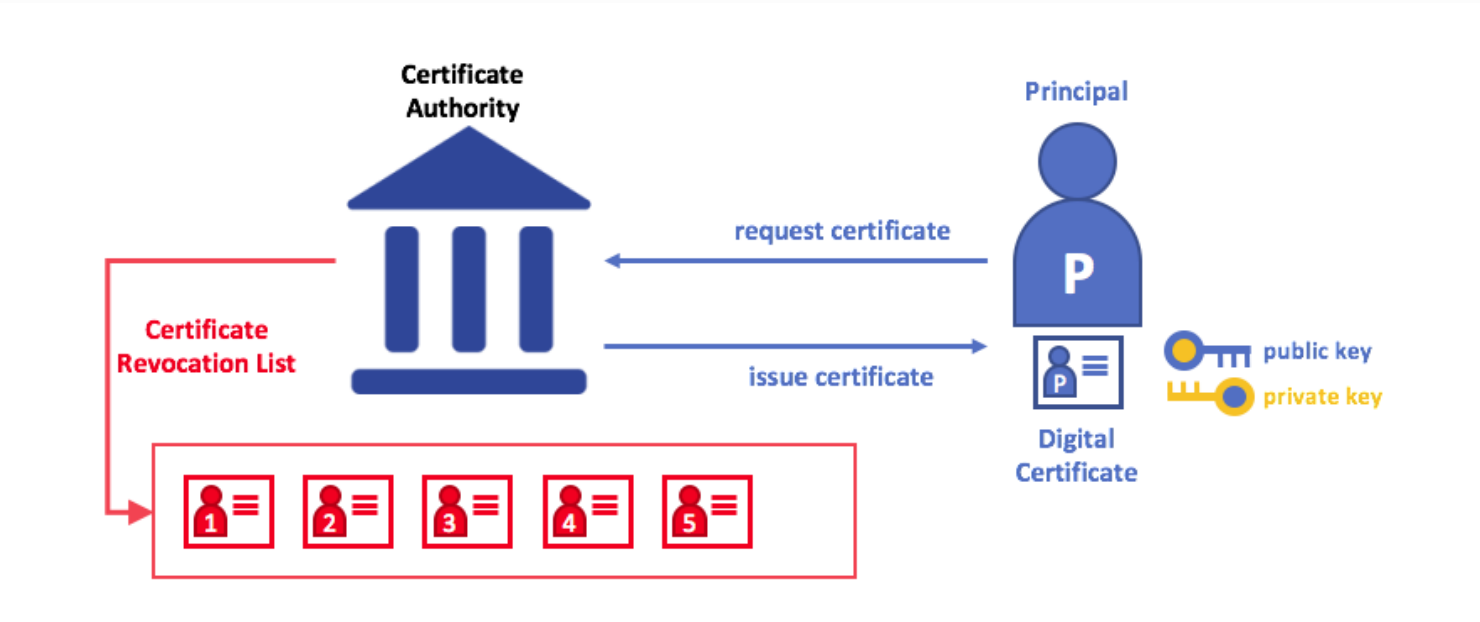
拥有有效的信用卡是不够的，它也必须被商店接受！PKI 和 MSP 以相同的方式协同工作，PKI提供身份列表，MSP说哪些是参与网络的给定组织的成员。

PKI 证书和 MSP 提供了类似的功能组合。PKI 就像一个卡片提供商，它分配了许多不同类型的可验证身份。另一方面，MSP 类似于商店接受的卡提供商列表，确定哪些身份是商店支付网络的可信成员（参与者）。**MSP 将可验证的身份转变为区块链网络的成员** 。

让我们更详细地深入研究这些概念。

什么是 PKI?

公钥基础结构（PKI）是一组互联网技术，可在网络中提供安全通信。是 PKI 将 **S** 放在 **HTTPS** 中，如果你在网页浏览器上阅读这个文档，你可能正使用 PKI 来确保它来自一个验证过的来源。



公钥基础结构（PKI）的元素。PKI 由向各方（例如，服务的用户，服务提供者）发布数字证书的证书授权中心组成，然后使用它们在与其环境交换的消息中对自己进行身份验证。CA 的证书撤销列表（CRL）构成不再有效的证书的参考。证书的撤销可能由于多种原因而发生。例如，因为与证书相关联的加密私有材料已被公开，所以证书可能被撤销。

虽然区块链网络不仅仅是一个通信网络，但它依赖于 PKI 标准来确保各个网络参与者之间的安全通信，并确保在区块链上发布的消息得到适当的认证。因此，了解 PKI 的基础知识以及为什么 MSP 是非常重要的。

PKI 有四个关键要素：

- **数字证书**
- **公钥和私钥**
- **证书授权中心**
- **证书撤销列表**

让我们快速描述这些 PKI 基础知识，如果你想了解更多细节，维基百科是一个很好的起点。

数字证书

数字证书是包含与证书持有者相关的属性的文档。最常见的证书类型是符合 X.509标准的证书，它允许在其结构中编码一些用于身份识别的信息。

例如，密歇根州底特律的 Mitchell 汽车的制造部门的 Mary Morris 可能有一个带有 `SUBJECT` 属性为 `C=US`，`ST=Michigan`，`L=Detroit`，`O=Mitchell Cars`，`OU=Manufacturing`，`CN=Mary Morris /UID=123456` 的数字证书。Mary 的证书类似于她的身份证（提供了 Mary 的信息），她可以用来证明关于她的重要事实。X.509 证书中还有许多其他属性，但现在让我们专注于这些。

描述一个名为 Mary Morris 的组织的数字证书。Mary 是证书的 `SUBJECT`*，突出显示的* `SUBJECT` *文本显示了关于 Mary 的重要事实。如你所见，证书还包含更多信息。最重要的是，Mary 的公钥是在她的证书中分发的，而她的私人签名密钥则不是。此签名密钥必须保密。*

重要的是，Mary 的所有属性都可以使用称为密码学（字面意思，“*秘密书写*”）的数学技术进行记录，这样篡改将使证书无效。只要对方信任证书颁发者，即**证书授权中心（CA）**，密码学就允许 Mary 将证书提交给其他人以证明其身份。只要 CA 安全地保存某些加密信息（CA 的**私钥**），任何阅读证书的人都可以确定有关 Mary 的信息没有被篡改，它将始终具有 Mary Morris 的特定属性。将 Mary 的 X.509 证书视为无法改变的数字身份证。

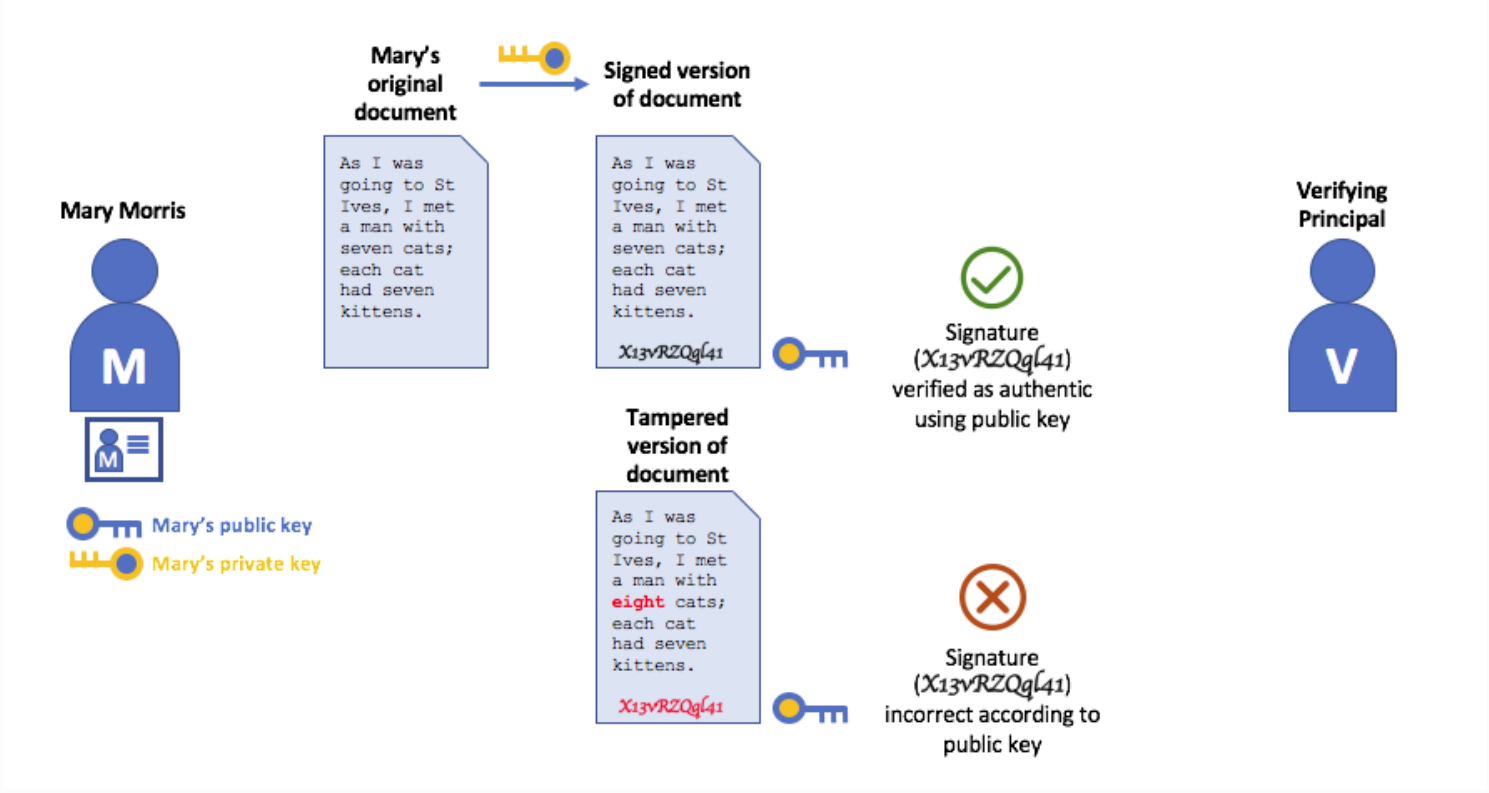
授权，公钥和私钥

身份验证和消息完整性是安全通信中的重要概念。身份验证要求确保交换消息的各方创建特定消息的身份。对于具有“完整性”的消息意味着在其传输期间不能被修改。例如，你可能希望确保与真正的 Mary Morris 而不是模仿者进行沟通。或者，如果 Mary 向你发送了一条消息，你可能希望确保其在传输过程中没有被其他任何人篡改过。

传统的身份验证机制依赖于**数字签名**，顾名思义，它允许一方对其消息进行数字**签名**。数字签名还可以保证签名消息的完整性。

从技术上讲，数字签名机制要求每一方保存两个加密连接的密钥：广泛可用的公钥和充当授权锚的私钥，以及用于在消息上产生**数字签名**的私钥 。数字签名消息的接收者可以通过检查附加签名在预期发送者的公钥下是否有效来验证接收消息的来源和完整性。

私钥和公钥的唯一关系是保证安全通信的加密魔法。密钥之间唯一的数学关系使得私钥在消息上的签名，只有对应公钥在相同的消息上才可以与之匹配。

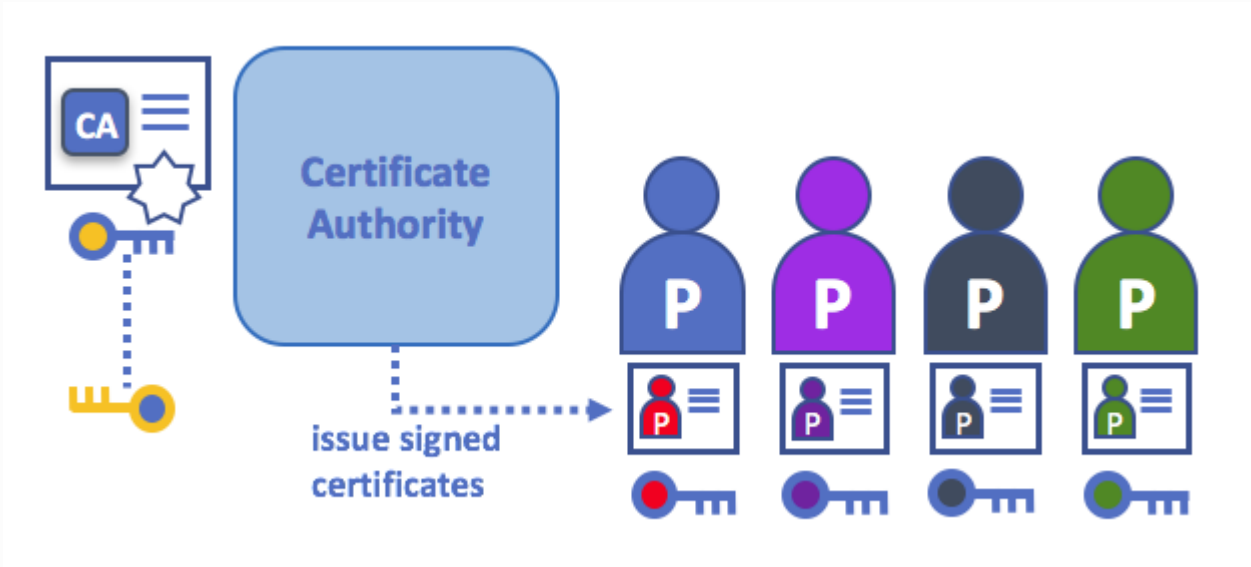


在上面的示例中，Mary 使用她的私钥对邮件进行签名。任何使用她的公钥查看签名消息的人都可以验证签名。

证书授权中心

如你所见，人员或节点能够通过由系统信任的机构为其发布的**数字身份**参与区块链网络。在最常见的情况下，数字身份（或简称**身份**）的形式为，符合 X.509 标准并由证书授权中心（CA）颁发的经加密验证的数字证书。

CA 是互联网安全协议的常见部分，你可能已经听说过一些比较流行的协议：Symantec（最初是 Verisign），GeoTrust，DigiCert，GoDaddy 和 Comodo 等。



证书授权中心向不同的参与者颁发证书。这些证书由 CA 进行签名，并将参与者的公钥绑定在一起（并且可选是否具有全部属性列表）。因此，如果一个成员信任 CA（并且知道其公钥），则可以信任与参与者绑定的证书中包含的公钥，并通过验证参与者证书上的 CA 签名来获取所包含的属性。

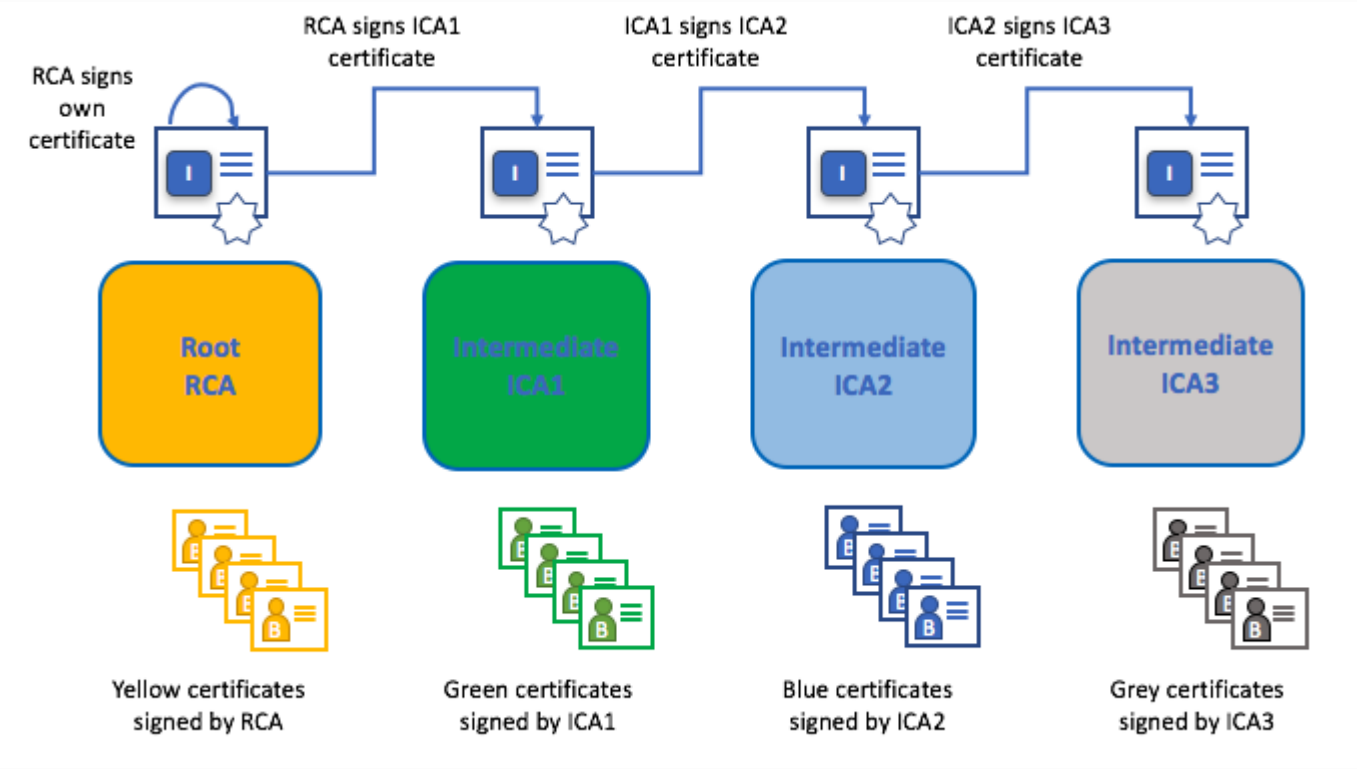
证书可以广泛传播，因为它们既不包括参与者也不包括 CA 的私钥。因此，它们可以用作信任的锚，用于验证来自不同参与者的消息。

CA 也有一个证书，它们可以广泛使用。这就可以让从给定 CA 获取身份证书的消费者验证自己的身份，因为只有对应的私钥才可以生成该证书。

在区块链设置中，希望与网络交互的每个参与者都需要一个身份。在此设置中，你可能会说使用**一个或多个 CA 从数字角度定义了组织的成员** 。CA 是为组织的参与者提供可验证的数字身份的基础。

根 CA，中间 CA 和信任链

CA 有两种形式：**根 CA**和**中间 CA** 。因为根 CA（Symantec，Geotrust等）*必须*安全地向互联网用户**颁发**数亿个证书，所以将这个过程分散到所谓的*中间 CA 中*是很有用的。这些中间 CA 具有由根 CA 或其他中间 CA 颁发的证书，允许为链中的任何 CA 颁发的任何证书建立“信任链”。追溯到根 CA 的能力不仅让 CA 的功能在仍然提供安全性的同时进行扩展（允许使用证书的组织充满信心地使用中间 CA），还限制了根 CA 的暴露，如果根 CA 受到损害，将会危及整个信任链。另一方面，如果中间 CA 受到损害，则曝光量会小得多。



只要每个中间 CA 的证书的颁发 CA 是根 CA 本身或具有对根 CA 的信任链，就在根 CA 和一组中间 CA 之间建立信任链。

中间 CA 在跨多个组织颁发证书时提供了巨大的灵活性，这在许可的区块链系统（如Fabric）中非常有用。例如，你将看到不同的组织可能使用不同的根 CA，或者使用具有不同中间 CA 的相同根 CA，这取决于网络的需求。

Fabric CA

因为 CA 非常重要，Fabric 提供了一个内置的 CA 组件，允许在你的区块链网络中创建 CA。此组件称为 **Fabric CA** ，是一个私有根 CA 提供者，能够管理具有 X.509 证书形式的 Fabric 参与者的数字身份。由

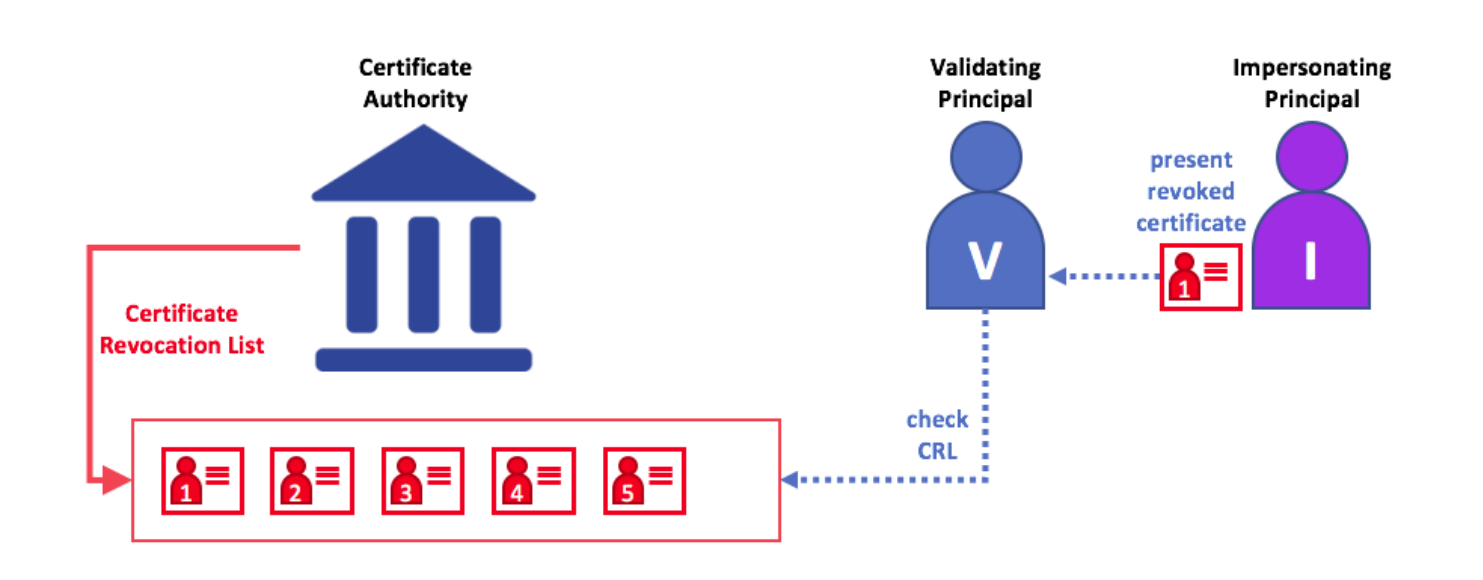
于 Fabric CA 是针对 Fabric 的根 CA 需求的自定义 CA，因此它本身无法为浏览器中的常规或自动使用提供 SSL 证书。但是，由于**一些** CA 必须用于管理身份（即使在测试环境中），因此可以使用 Fabric CA 来提供和管理证书。使用公共或商业的根或中间 CA 来提供识别也是可以的，并且完全合适。

如果你有兴趣，你可以在 CA 文档部分阅读有关 Fabric CA 的更多信息。

证书撤销列表

证书撤销列表（Certificate Revocation List，CRL）很容易理解，它是 CA 知道由于某些原因而被撤销的证书的引用列表。如果你回想商店场景，CRL 就像被盗信用卡列表一样。

当第三方想要验证另一方的身份时，它首先检查颁发 CA 的 CRL 以确保证书尚未被撤销。验证者不是必须要检查 CRL，但如果不检查，则他们冒着接受无效身份的风险。



使用 CRL 检查证书是否仍然有效。如果模仿者试图将无效的数字证书传递给验证者，则可以首先检查颁发证书的 CA 的 CRL，以确保其未被列为无效。

请注意，被撤销的证书与证书过期非常不同。撤销的证书尚未过期，按其他方式来说，它们是完全有效的证书。有关 CRL 的更多深入信息，请单击 此处。

现在你已经了解了 PKI 如何通过信任链提供可验证的身份，下一步是了解如何使用这些身份来代表区块链网络的可信成员。这就是 MSP 发挥作用的地方——**它确定了区块链网络特定组织的成员**。

要了解有关成员的更多信息，请查看有关 MSP的概念文档。