数字签名是用于验证数字数据的真实性和完整性的加密机制。我们可能会认为它是常见手写签名的数字版本，但是它更复杂，更安全。

简而言之，数字签名是附加在消息或文档上的一段代码。生成代码后，可以证明该消息在从发送方发送到接收方时未被篡改。

通过加密保护通信的概念可以追溯到远古时代，但是随着1970年代公钥加密(PKC)的发展，数字签名方案成为可能。因此，要了解数字签名的工作方式，您首先需要了解哈希函数和公共密钥密码学的基础知识。

哈希函数

散列是数字签名系统的关键元素之一。散列涉及将任何大小的数据转换为固定大小的值。这是通过称为哈希函数的特殊算法完成的。哈希函数产生的结果值称为哈希值或消息摘要。

当与加密结合使用时，可以使用所谓的加密哈希函数来生成可用作唯一数字指纹的哈希值(摘要)。这意味着输入数据(消息)的任何更改都将导致完全不同的结果(哈希值)。这就是为什么加密哈希函数被广泛用于验证数字数据的真实性的原因。

公钥密码术(PKC)

公钥密码术(PKC)是指使用一对密钥组成的加密系统，该密钥对包括一个公钥和一个私钥。这两个密钥在数学上相关，并且可以用于数据加密和数字签名。

作为一种加密工具，PKC

比最基本的方法对称加密更安全。较早的系统需要相同的密钥来加密和解密信息，但是PKC使用公共密钥加密数据，并使用相应的私有密钥进行数据解密。

此外，PKC方案可以应用于数字签名生成。基本上，这涉及通过签名者的私钥对消息(或数字数据)进行哈希处理。然后，邮件收件人可以使用签名者提供的公共密钥来验证签名是否有效。

在某些情况下，数字签名可能包括加密，但并非总是如此。例如，比特币区块链使用PKC和数字签名，但是与许多人相反，该过程不包括加密。严格来说，比特币使用椭圆曲线数字签名算法(ECDSA)来验证交易。

如何制作数字签名?

在加密世界中，数字签名系统通常包含三个基本步骤：哈希，签名和验证。

数据散列

第一步是对消息或数字数据进行哈希处理。这是通过使用哈希算法提交数据以生成哈希值(例如，消息摘要)来完成的。如前所述，消息大小可以有很大的不同，但是当进行散列处理时，它们将具有相同长度的散列。这是哈希函数的最基本属性。

但是，对数据进行哈希处理以生成数字签名不是必需的，您还可以使用私钥对根本没有哈希的消息进行签名。但是，在使用加密货币的情况下，总是对数据进行哈希处理，因为处理固定长度的摘要会简化整个过程。

签名

对信息进行哈希处理后，需要消息发送者的签名。这是使用公钥加密的时刻。数字签名算法有很多不同的类型，每种都有自己的机制。但是，默认情况下，散列消息使用私钥签名，并且邮件收件人可以使用相应的公共密钥(由签名者提供)进行验证。

换句话说，如果在生成签名时不包括私钥，则邮件接收者将无法使用相应的公钥来对其进行验证。公钥和私钥都是由消息发送者生成的，但是只有公钥才与收件人共享。

重要的是要注意，数字签名与每个消息的内容直接相关。因此，与手写签名不同，每个数字签名的消息将具有不同的数字签名。

验证

让我们以一个示例来说明最终验证阶段的整个过程。假设爱丽丝(Alice)向鲍勃(Bob)写了一条消息，对其进行了哈希处理，然后根据哈希值和私钥生成了数字签名。该签名将用作特定消息的唯一数字指纹。

Bob收到消息后，可以使用Alice的公钥来验证数字签名。这样，Bob可以确保签名是由Alice生成的，因为只有Alice(至少，正如我们期望的那样)具有与公钥相对应的私钥。

结果，爱丽丝必须保持她的私钥安全。如果有人获得了爱丽丝的私钥，则可以生成

数字签名并假装为爱丽丝。就比特币而言，这意味着有人可以在未经许可的情况下移动或使用爱丽丝的比特币。

为什么数字签名很重要?

数字签名通常用于实现三个结果：数据完整性，真实性和不可否认性。

数据完整性：Bob可以验证传输过程中Alice的消息没有更改。如果消息被修改，将生成完全不同的签名。

真实性：只要保持爱丽丝的私钥安全，鲍勃就可以验证数字签名是由爱丽丝而不是其他任何人生成的。

不可否认性：除非出于某些特定原因公开了爱丽丝的私钥，否则一旦生成签名，爱丽丝将无法否认他或她已经对其进行签名。

应用实例

数字签名可以应用于各种数字文档和证书。因此，数字签名以多种方式使用，最常见的用例是：

信息技术：用于增强Internet通信系统的安全性。

财务：数字签名可用于审计，费用报告，贷款协议等。

法律：数字签名可用于所有类型的商业和法律协议，包括政府文件。

医疗：数字签名可用于防止虚假处方和医疗记录。

区块链：数字签名方案确保只有那些拥有加密货币合法所有权的人(除非私钥被泄露)才能签署交易以进行资金转移。

余量

数字签名方案面临的主要挑战来自三个最低要求。

算法：数字签名方案中使用的算法级别很重要。这包括选择一个受信任的哈希函数和一个加密系统。

实现：如果算法不错，但实现不好，则数字签名系统将存在缺陷。

私钥：如果私钥泄漏或被泄露，则真实性和不可否认属性将不再有效。如果加密货币用户丢失其私钥，则可能导致重大的财务损失。

数字签名与数字签名

简而言之，数字签名与某些类型的电子签名相关联，这意味着如何对文档和消息进行电子签名。因此，所有数字签名都是电子签名，但是电子签名并不总是数字签名。

它们之间的主要区别在于身份验证方法。数字签名使用加密系统，例如哈希函数，公共密钥密码学和密码学。

最后

哈希函数和公共密钥密码术是数字签名系统的核心，并在当今广泛的应用中得到使用。正确实施后，数字签名可以提高安全性，确保完整性并启用任何类型的数字数据的身份验证。

在区块链世界中，数字签名用于签署和批准加密货币交易。该签名在比特币中尤其重要，因为只有拥有相应私钥的人才能使用该硬币。

电子签名和数字签名已经使用了很多年，但是仍有很大的增长空间。当今，许多官僚机构仍以书面工作为基础，但是随着我们转向更数字化的系统，将会采用更多的数字签名方案。