Abstract：区块链是一种基于互联网的技术，它可以追究商品溯源、辨别真伪、保护网络安全。在这个网络犯罪诈骗泛滥的时代，密码被盗用成为了犯罪最常见的手段。

区块链是一种基于互联网的技术，它可以追究商品溯源、辨别真伪、保护网络安全。在这个网络犯罪诈骗泛滥的时代，密码被盗用成为了犯罪最常见的手段。那么，区块链技术可以让密码变得更安全吗？这就涉及到了区块链的密码学。

信息安全及密码学技术，是整个信息技术的基石。在区块链中，也大量使用了现代信息安全和密码学的技术成果，主要包括：哈希算法、对称加密、非对称加密、数字签名、数字证书、同态加密、零知识证明等。本章从安全的完整性、机密性、身份认证等维度，简要介绍区块链中安全及密码学技术的应用。·完整性（防篡改）区块链采用密码学哈希算法技术，保证区块链账本的完整性不被破坏。

哈希（散列）算法能将二进制数据映射为一串较短的字符串，并具有输入敏感特性，一旦输入的二进制数据，发生微小的篡改，经过哈希运算得到的字符串，将发生非常大的变化。

此外，优秀哈希算法还具有冲突避免特性，输入不同的二进制数据，得到的哈希结果字符串是不同的。区块链利用哈希算法的输入敏感和冲突避免特性，在每个区块内，生成包含上一个区块的哈希值，并在区块内生成验证过的交易的 Merkle 根哈希值。

一旦整个区块链某些区块被篡改，都无法得到与篡改前相同的哈希值，从而保证区块链被篡改时，能够被迅速识别，最终保证区块链的完整性（防篡改）。

机密性加解密技术从技术构成上，分为两大类：一类是对称加密，一类是非对称加密。对称加密的加解密密钥相同；而非对称加密的加解密密钥不同，一个被称为公钥，一个被称为私钥。公钥加密的数据，只有对应的私钥可以解开，反之亦然。区块链尤其是联盟链，在全网传输过程中，都需要 TLS(Transport Layer Security)加密通信技术，来保证传输数据的安全性。

而 TLS 加密通信，正是非对称加密技术和对称加密技术的完美组合：通信双方利用非对称加密技术，协商生成对称密钥，再由生成的对称密钥作为工作密钥，完成数据的加解密，从而同时利用了非对称加密不需要双方共享密钥、对称加密运算速度快的优点。身份认证单纯的 TLS 加密通信，仅能保证数据传输过程的机密性和完整性，但无法保障通信对端可信（中间人攻击）。因此，需要引入数字证书机制，验证通信对端身份，进而保证对端公钥的正确性。

数字证书一般由权威机构进行签发。通信的一侧持有权威机构根CA(Certification Authority)的公钥，用来验证通信对端证书是否被自己信任（即证书是否由自己颁发），并根据证书内容确认对端身份。在确认对端身份的情况下，取出对端证书中的公钥，完成非对称加密过程。

此外，区块链中还应用了现代密码学最新的研究成果，包括同态加密、零知识证明等，在区块链分布式账本公开的情况下，最大限度地提供隐私保护能力。这方面的技术，还在不断发展完善中。

区块链安全是一个系统工程，系统配置及用户权限、组件安全性、用户界面、网络入侵检测和防攻击能力等，都会影响最终区块链系统的安全性和可靠性。区块链系统在实际构建过程中，应当在满足用户要求的前提下，在安全性、系统构建成本以及易用性等维度，取得一个合理的平衡。