**3.（选作）调研国标GM/T0004-2012**

GM/T0004-2012是中国国家密码管理局于2012年发布的密码行业标准，正式名称为《SM3密码杂凑算法》。该标准定义了SM3哈希算法的技术细节，广泛应用于数字签名、消息认证码（MAC）生成与验证、随机数生成等密码学应用中。

**SM3算法简介**

（1）输出长度：256位（32字节）

（2）输入限制：最大支持264位的输入

（3）结构设计：采用Merkle–Damgård构造，类似于SHA-256，但具有独特的消息扩展机制和压缩函数设计

（4）应用场景：广泛用于电子政务、金融、电信等对信息安全要求较高的领域

**4.（选作）调研区块链中Merkletree的作用，是否可以直接将所有交易信息输入某hash算法，hash值放在区块中？为什么？**

（1）Merkle树在区块链中的作用

**1.高效验证交易存在性（Merkle证明）**  
 Merkle树允许通过“Merkle证明”验证某笔交易是否包含在某个区块中，而无需下载整个区块的数据。这种验证过程只需提供从目标交易到Merkle根的路径上的哈希值，验证所需的数据量是对数级别的，极大地提高了验证效率。

**2.支持轻节点（SPV）操作**  
 轻节点（如移动钱包）不需要存储完整的区块链数据。通过Merkle树，轻节点可以仅凭区块头中的Merkle根和相关的Merkle证明，验证特定交易的存在性，从而实现资源高效的操作。

**3.增强数据完整性和安全性**  
 Merkle树的结构确保了交易数据的不可篡改性。任何对交易数据的修改都会导致相应的哈希值变化，进而影响到Merkle根的值，使得篡改行为易于被检测。

（2）不能仅使用所有交易的单一哈希值。原因如下：

**1.缺乏高效的交易验证机制**  
 如果仅将所有交易数据合并后计算一个哈希值（例如将所有交易数据串联后进行哈希），那么验证某笔交易是否包含在区块中就需要访问整个交易集合。这种方法在数据量大时效率低下，尤其不适合资源受限的设备。

**2.无法支持轻节点的操作**  
 轻节点依赖于Merkle证明来验证交易的存在性。如果没有Merkle树结构，轻节点将无法在不下载完整区块的情况下进行验证，限制了其在区块链网络中的功能。

**3.增加数据同步和验证的复杂性**  
 在节点之间同步数据时，Merkle树允许通过比较Merkle根快速检测数据差异，进而只同步有差异的部分。而使用单一哈希值的方法则无法实现这种高效的数据同步机制。