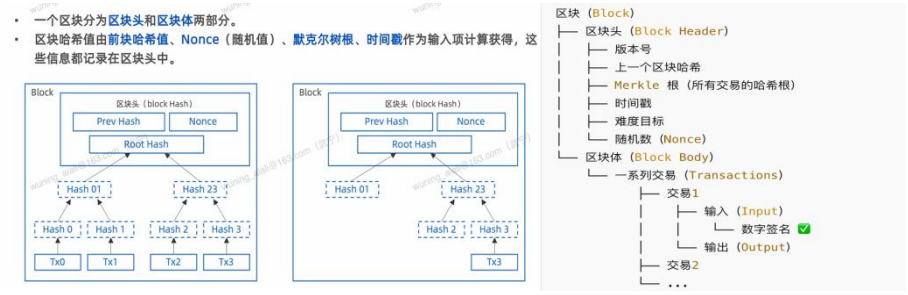
共识机制：PoW - 谁先破解区块 Hash 谁拥有记账权。

区块的链式存储结构：

区块内部结构：



核心算法：

算法 1：

HASH：SHA256 算法是 Hash 函数的一种，把**任意长度的输入**通过散列算法转换成**固定长度的输出；**Hash 函数是防碰撞的，只有相同的输入才会有相同的输出。HASH 算法还包含 MD5、SHA-1、SHA-256、SHA-3、Blake2 等，加密特点：不可逆。即原文经加密算法加密后，无法反向从秘文解密到原文。

举例：

矿工需要不断尝试随机数（Nonce）找到目标 HASH 值。目标 HASH 值是由系统根据 前一个 block 的 hash + Nonce + Merkle 树根 + Timestamp，其中前一个 block 的 hash、Merkle 树根是已知的，只需要猜中 Nonce 和 Timestamp，在 Nonce 穷尽完成后依然无法破解 HASH 时，矿工通常会调整 Timestamp 再次进行 HASH 破解。

算法 2：

数字签名算法：数字签名技术验证数据修改权限，数字签名可以验证数据持有者的身份，确保只有持有私钥的用户才可以对数据进行修改。私钥持有者可以编辑 Input 数据，验证者只能通过网络中公钥读取数据。加密特点：非对称加密算法，公钥私钥共同配合加解密（公钥加密，私钥解密 或 私钥加密，公钥解密），btc 采用的是 ECDSA 算法。互联网最典型的算法：RSA，网站的 https 协议中 SSL 协议层即采用 RSA 非对成加密算法完成数据从浏览器到服务器的网络安全传输，浏览器使用网络中的公钥对数据加密，服务端使用私钥对数据进行解密。

举例：

A 发起一笔交易（如：转账 1 BTC 给别人），A 用 A 的私钥对交易内容进行签名，网络上所有人用 A 的公钥验证签名，验证通过 → 交易有效，验证失败 → 拒绝打包进区块。

```
[交易内容] + [私钥签名] → 签名数据
→ 广播到比特币网络
→ 所有节点使用你的公钥验证签名
→ 验证成功 → 交易有效
```