1、ECDSA 简介

ECDSA（Elliptic Curve Digital Signature Algorithm，椭圆曲线数字签名算法）是一种基于椭圆曲线密码学的非对称加密算法，用于生成和验证数字签名。下面是 ECDSA 的算法描述与原理：

1. **参数设置：**
   - 选择一个椭圆曲线方程，通常为 secp256k1。
   - 确定一个基点 G，它是椭圆曲线上的一个固定点。
   - 确定一个大素数 n，它是椭圆曲线上的一个循环群的阶。
2. **密钥生成：**
   - 生成一个私钥 d，它是一个 256 位的随机数。
   - 使用私钥 d 计算公钥 Q = d * G，其中 * 表示椭圆曲线上的点乘法。公钥 Q 是一个椭圆曲线上的点。
3. **签名生成：**
   - 假设要对消息 m 进行签名。
   - 选择一个随机数 k，满足 1 ≤ k < n。
   - 计算点 R = k * G，并将 R 的 x 坐标（记作 r）取模 n。
   - 计算 s = (hash(m) + d * r) / k mod n，其中 hash()是一个哈希函数。s 是签名的一部分。
4. **签名验证：**
   - 假设收到一条消息 m 和它的签名(r, s)。
   - 验证 r 和 s 是否在 0 到 n-1 的范围内。
   - 计算点 R' = (s^-1 * hash(m) * G + s^-1 * r * Q)，其中 s^-1 是 s 的模 n 的逆元。
   - 验证 R'的 x 坐标是否等于 r。如果相等，则签名有效。

ECDSA 的安全性基于椭圆曲线上的离散对数问题的困难性。私钥 d 是难以通过公钥 Q 计算得到的，因此保证了私钥的安全性。同时，签名的验证过程能够确保签名的完整性和认证发送者身份。需要注意的是，ECDSA 算法中的随机数 k 的选择非常重要，如果 k 被多个消息重复使用，私钥可能会暴露。因此，在实际应用中，需要使用密码学安全的伪随机数生成器来生成 k。此外，ECDSA 还需要使用适当的哈希函数来计算消息的哈希值。

2、推导技术

在以太坊中，ECDSA（椭圆曲线数字签名算法）是用于对交易进行数字签名的算法。推导技术是一种利用已知信息和算法进行推理的方法,可用于从相关数据中推导出隐藏的信息或者密钥。推导技术在以太坊的 ECDSA 中有以下几个应用：

1. **私钥推导：**以太坊中的钱包通常使用助记词（Mnemonic）来生成私钥。通过一系列的推导算法,可以从助记词推导出对应的私钥。这种推导技术可以方便地从助记词恢复私钥，而不需要直接存储私钥。

2. **公钥推导：**通过私钥可以推导出对应的公钥。在以太坊中，用于验证 ECDSA 签名的公钥是从私钥推导得到的。推导公钥的过程涉及到椭圆曲线上的点乘运算，通过私钥和基点（G）进行点乘运算即可得到公钥。

3. **地址推导：**在以太坊中，地址是由公钥经过一系列运算得到的。首先，对公钥进行 Keccak-256 哈希运算，然后取哈希结果的后 20 个字节作为地址。地址推导的过程可以通过

对公钥进行哈希运算来实现。

4. 智能合约推导：在以太坊中，智能合约也可以通过推导技术进行创建和部署。通过对已部署合约的字节码进行推导和解析，可以获得合约的代码、状态和功能。

推导技术在以太坊的 ECDSA 中起到了关键作用，可以方便地生成和恢复私钥、公钥和地址，同时也便于智能合约的创建和部署。

3、参考文献

【1】https://zhuanlan.zhihu.com/p/31671646
【2】Elliptic Curve Digital Signature Algorithm - Wikipedia