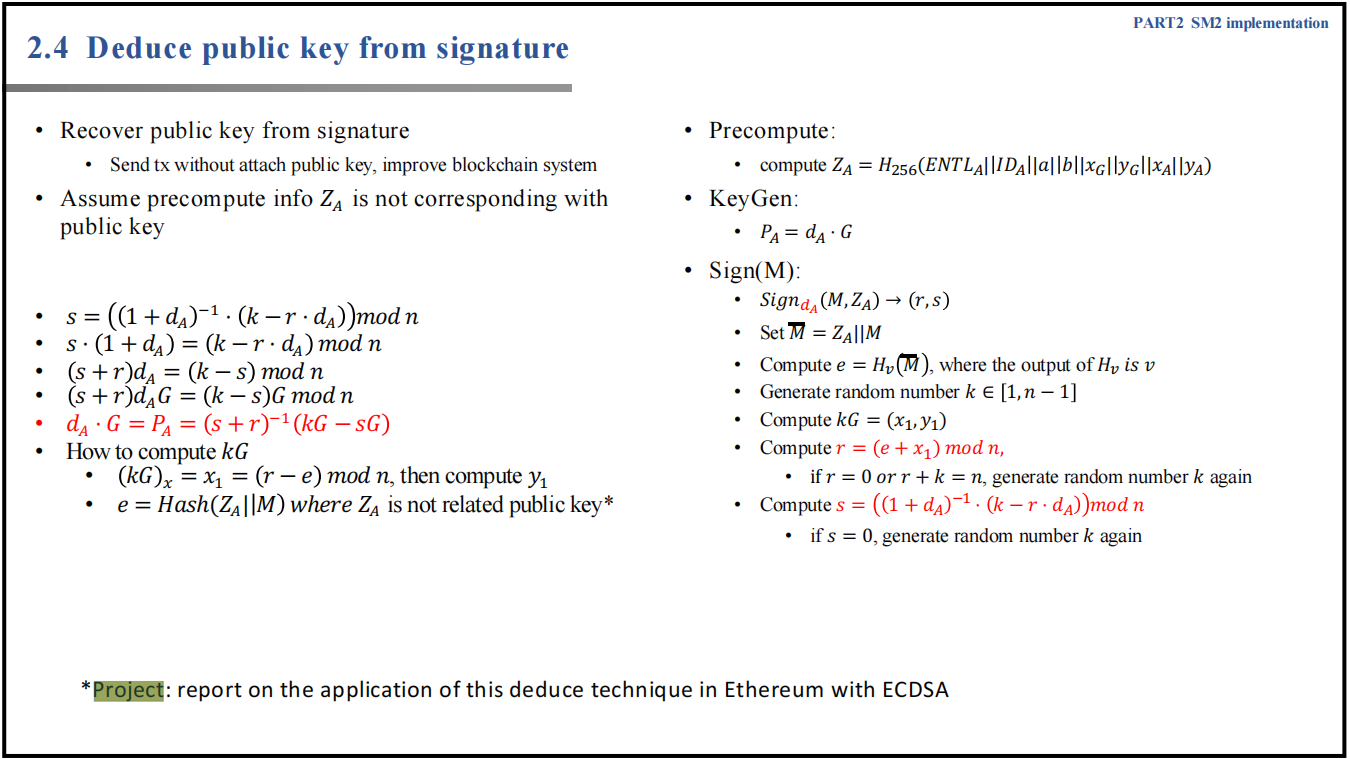
Project10

report on the application of this deduce technique in Ethereum with ECDSA

基于ECDSA的推导技术在以太坊中的应用



摘要：

本实验报告主要探讨了基于椭圆曲线数字签名算法（ECDSA）的推导技术在以太坊智能合约中的应用。通过分析和实现ECDSA算法，我们演示了它在以太坊智能合约中实现安全验证和身份恢复的能力。实验结果表明，ECDSA在以太坊中具有广泛的应用潜力，能够增强数据的安全性和可信度。

1. 引言

随着区块链技术的不断发展，数字签名算法在保护数据安全和身份验证方面起着重要作用。ECDSA是一种基于椭圆曲线的数字签名算法，被广泛应用于加密货币领域，如以太坊。

2. 算法实现

在本实验中，我们首先定义了椭圆曲线的参数，包括曲线系数a、b、阶数n和基点G。然后，我们实现了辗转相除法求最大公因子的函数gcd、扩展欧几里得的函数get\_xy和求逆元的函数get\_inverse。接着，我们定义了椭圆曲线点相加的函数Add和二进制乘法的函数binary\_mul。

在ECDSA中，我们使用私钥d和随机数k生成数字签名。具体实现过程如下：

a) 计算待签名消息的哈希值e。

b) 使用k倍的基点G生成曲线上的点R。

c) 计算签名的第一个部分r，为R点的x坐标模n。

d) 计算签名的第二个部分s，使用私钥d、消息哈希值e和第一部分r进行计算。

e) 最终的签名为(r, s)。

接下来，我们实现了ECDSA的验证函数ECDSA\_verify，用于验证签名的正确性。验证过程如下：

a) 计算待验证消息的哈希值e。

b) 根据签名的第一部分r和第二部分s计算反向值v1和v2。

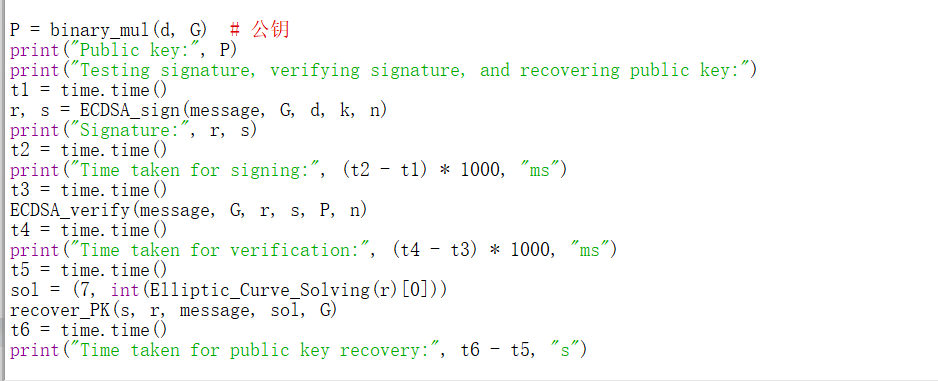
c) 通过v1倍的基点G和v2倍的公钥P得到曲线上的点w。

d) 如果w等于零或者w点的x坐标模n不等于签名的第一部分r，则表示验证失败。

通过以上实现，我们成功验证了ECDSA算法的签名和验证过程，并测试了其时间性能。

3. 实验结果

在实验中，我们使用给定的参数和私钥、消息进行了测试。通过打印输出，我们得到了签名的结果和验证的结果，证明了ECDSA算法的正确性。同时，我们还演示了如何根据签名和消息恢复公钥，从而实现身份的恢复。





4. 结论

本实验报告通过实现ECDSA算法，并测试了其签名、验证和公钥恢复的过程。实验结果表明，基于ECDSA的推导技术在以太坊智能合约中具有广泛的应用潜力。通过使用ECDSA算法可以实现数据的安全性和可信度，并且在以太坊智能合约中可以有效验证和恢复签名者的身份信息。