# 摘要

略略略

**关键词：**门限签名，盲签名，ECDSA，同态加密

# ABSTRACT

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.……

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.……

……

**Key words:** Threshold Signature, Blind Signature, ECDSA, Homomorphic Encryption

# 目录

# 绪论

## 论文研究背景及意义

随着区块链技术的发展和普及，这项技术已经产生了多种多样的应用。随之而来的是越来越多的用户开始涉足区块链世界。他们通过使用公私钥进行数字签名来发起交易并参与区块链网络的运作。为了使用户更便利地管理其数字资产，数字钱包等产品应运而生，成为用户与区块链之间的桥梁。然而，随着区块链技术的普及和用户群体的扩大，安全隐患也逐渐暴露出来。

遗失私钥或私钥被黑客攻击是区块链用户面临的重大风险之一。许多用户可能因个人疏忽，如存储私钥的不当或遗忘备份等，而导致私钥丢失，从而失去对其链上资产的所有权。更为严重的是，黑客可能利用各种技术手段入侵数字钱包或交易所，窃取用户的私钥，进而窃取用户的数字资产，给用户带来巨大的经济损失。//数据或新闻引用

这些恶意事件的发生凸显了当前数字资产管理和交易过程中的安全性问题。用户对于自身数字资产的安全性越来越关注，迫切需要更加可靠和安全的解决方案来保护其资产免受损失。因此，区块链技术领域亟需加强安全意识和技术防范手段的研发，以应对不断演变的安全威胁，为用户提供更加可靠的数字资产保障。