区块链数字钱包安全性分析与数字签名方案设计

Security Analysis of Blockchain Digital Wallet and Design of Digital Signature Scheme

分类号_____ 密级_____
UDC _____ 编号_____

硕 士 学 位 论 文

学位论文题目： 区块链数字钱包安全性分析与数字签名方案设计

姓　　名 方李西

学　　号 2020212340

学　　院 信息学院

学位类别： ☑ 学术硕士 □专业硕士 □同等学力

学科专业 网络空间安全

指导教师 朱建明

第二导师 _____

提交论文日期：　　2022 年 5 月 22 日

摘要

近些年来，随着比特币、以太坊等加密数字货币的发展，区块链技术受到各界的广泛关注和国家政策的大力支持。在2021年颁布的“十四五规划和2035年远景目标纲要”中，提出加快推动区块链技术应用。与此同时，货币资产存储和交易的需求量快速增长，作为存储数字货币的设备，数字钱包的使用范围也在不断扩大。但是，由于区块链技术还处于快速发展阶段，区块链系统仍然存在一些漏洞，攻击者可利用这些漏洞发起攻击，对数字货币和数字钱包造成严重威胁。

在数字钱包中，密钥有着非常重要的作用，通过公钥可以发起转账、查询交易等功能，而私钥代表数字货币的拥有权。在传统数字钱包中，密钥一般集中存储在本地数据库或者第三方平台的服务器上。攻击者一旦获取私钥存储的具体位置，可以发起单点攻击造成节点故障，从而窃取数字资产。基于此，本文研究区块链数字钱包的安全性与数字签名方案，具体研究工作如下：

（1）对区块链数字钱包进行安全性分析。按照私钥存储位置和私钥使用方式对数字钱包分类，分成软件钱包、硬件钱包等6类，对比这6类钱包的优缺点以及安全性。数字钱包的运行依赖于区块链，因此从区块链安全着手，研究区块链系统安全以及数据安全。在区块链系统安全方面，以比特币系统和以太坊系统为例，描述并分析了7种攻击对区块链系统的影响。在数据安全方面，从交易数据安全的角度出发，分析现有的两种数据安全机制，分别为混币机制和加密技术，并介绍这两种机制的典型应用。

（2）提出了一种数字签名方案。本文针对传统数字钱包单点故障问题，设计了一种门限椭圆曲线方案，方案包括生成密钥、生成数字签名和验证数字签名三个阶段。从理论上，分析了方案的正确性和安全性，证明该方案在理论上是安全的。从实验上，通过计算开销和算法复杂度两个角度评估该方案的性能。

研究工作表明，对区块链数字钱包安全性分析，分析影响数字钱包安全性的因素，通过这些因素可以实现数字钱包方案间的安全性比较，为区块链数字钱包安全性比较提供思路。设计的门限签名方案相对于传统数字签名而言，能够抵抗合谋攻击，安全程度更高；方案中的椭圆曲线数字签名算法在经典椭圆曲线数字签名算法的基础上进行了改进，既能保证安全性又降低了算法复杂度，提高了签名的效率。

关键词：区块链；数字货币；数字钱包；安全性；椭圆曲线数字签名；

ABSTRACT

In recent years, with the development of encrypted digital currencies such as Bitcoin and Ethereum, blockchain technology has received extensive attention from all walks of life and strong support from national policies. In the "14th Five-Year Plan and 2035 Vision Outline" promulgated in 2021, it is proposed to accelerate the application of blockchain technology. At the same time, the demand for currency asset storage and trading is growing rapidly, and as a device for storing digital currency, the scope of use of digital wallets is also expanding. However, due to the rapid development of blockchain technology, there are still some loopholes in the blockchain system, which can be exploited by attackers to launch attacks, posing a serious threat to digital currencies and digital wallets.

In a digital wallet, the key plays a very important role. The public key can initiate transfers, query transactions and other functions, while the private key represents the ownership of the digital currency. In traditional digital wallets, keys are generally centrally stored in a local database or a server on a third-party platform. Once an attacker obtains the specific location where the private key is stored, he can launch a single-point attack to cause node failure, thereby stealing digital assets. Based on this, this paper studies the security and digital signature scheme of blockchain digital wallets. The specific research work is as follows:

(1) Security analysis of blockchain digital wallets. According to the storage location of the private key and the way of using the private key, the digital wallets are classified into 6 categories such as software wallets and hardware wallets, and the advantages, disadvantages and security of these 6 types of wallets are compared. The operation of digital wallets depends on the blockchain, so starting from the blockchain security, the blockchain system security and data security are studied. In terms of blockchain system security, taking the Bitcoin system and the Ethereum system as examples, the impact of seven attacks on the blockchain system is described and analyzed. In terms of data security, from the perspective of transaction data security, this paper analyzes two existing data security mechanisms, namely currency mixing mechanism and encryption technology, and introduces typical applications of these two mechanisms.

(2) A digital signature scheme is proposed. Aiming at the single point of failure problem of traditional digital wallets, this paper designs a threshold elliptic curve scheme. The scheme includes three stages: key generation, digital signature generation and digital signature verification. Theoretically, the correctness and security of the scheme are analyzed, and it is proved that the scheme is theoretically safe. Experimentally, the performance of this scheme is evaluated from the perspectives of computational overhead and algorithm complexity.

The research work shows that by analyzing the security of blockchain digital wallets and analyzing the factors that affect the security of digital wallets, the security comparison between digital wallet schemes can be achieved through these factors, which provides ideas for the security comparison of blockchain digital wallets. Compared with the traditional digital signature, the designed threshold signature scheme can resist collusion attacks and has a higher degree of security; the elliptic curve digital signature algorithm in the scheme is improved on the basis of the classic elliptic curve digital signature algorithm, which can not only ensure the security It reduces the complexity of the algorithm and improves the efficiency of the signature.

Key Words: Blockchain; Digital Currency; Digital Wallets; Safety; ECDSA

目　录

1 绪论

1.1 选题背景及意义

1.1.1 选题背景

（1） 区块链技术的发展

随着大数据、人工智能和云计算等技术的发展，数据安全已经严重影响人们的生活，保证数据安全迫在眉睫。区块链是一种将密码算法、点对点网络（P2P）、共识算法等多项技术交叉与融合的新技术，具有分布式存储、匿名性高和不可篡改等特点，促进数据共享和保证数据安全[1]。近些年来，区块链发展十分迅速，受到大众的广泛关注。在 2021 年颁布的“十四五规划和 2035 年远景目标纲要”中，将区块链作为新兴数字产业之一，提出加快推动区块链技术应用和产业发展的指导意见[2] 。

区块链的应用场景十分广泛，为推动产业数字化转型发挥巨大作用。到目前为止，区块链已经应用于金融、医疗、产品溯源等多个行业和领域[3-5]。在医疗行业中，由于医疗信息中包含大量的用户隐私数据，如何共享医疗数据的同时又能保证隐私数据的安全一直是医疗行业发展的难题。针对这一问题，Azeria 等人从处理电子医疗数据方法上进行创新，采用区块链技术，设计一种医疗数据管理系统 MedRec[6]。 MedRec 将电子医疗数据存储在一个综合日志上，通过公钥加密算法将访问权限分配给医院和患者，由医院和患者共同参与网络的维护，从而提高电子医疗数据的访问控制。在知识产权行业中，一些产权所有者将专利、著作等作品发布到知识产权区块链数据库上，通过区块链技术，生成的不可篡改的存在性证明，保护知识产权的安全 [7]。在市场需求和国家政策的双重支持下，食品溯源行业俨然成为当下热门行业之一。区块链具有不可伪造、可追溯的特性，将区块链技术应用在食品溯源行业中，能最大程度上解决数据的造假问题，增强食品安全的可信度[8]。

（2） 基于区块链的数字货币的兴起

虽然区块链应用场景广泛，但是应用最成熟的还是数字货币，区块链最初起源于比特币。2008 年 10 月，中本聪发表了一篇名为《比特币：一种点对点的电子现金系统》的论文，引起不少学者的关注[9] 。这篇论文详细介绍了如何在 P2P

网络中，设计一种去中心化的电子支付系统，这种支付系统和传统的基于信用模式的电子支付系统不同，它基于密码学原理，通过节点间达成一致共识，直接完成支付。这个电子现金系统也就是我们所说的比特币系统，比特币系统解决了传统支付系统高度中心化和缺乏信任度等问题。

比特币的出现，带动了去中心化支付系统的发展，市场上相继出现了很多基于区块链技术的加密数字货币，例如以太坊、莱特币、门罗币等。我国也正在不断推进数字货币的发展，目前也已推出法定数字货币 DCEP。并且在“十四五规划和 2035 年远景目标纲要”中明确提出稳妥推进数字货币的研发，加快金融机构数字化转型。

数字货币中使用非对称加密算法形成一系列的密钥对，私钥代表着交易者账户里的资产所有权。以比特币为例，比特币系统通过私钥确定用户身份，只有资产所有者拥有正确完整的私钥。例如交易者 A 向交易者 B 发起一笔交易，需要使用Pk_B进行加密，只有交易者 B 使用私钥解密，获得签名后的交易信息，完成资产的转移。如果用户私钥丢失或者被攻击者盗取，意味着私钥所对应的数字资产丢失。因此，确保用户私钥安全对保障数字资产安全具有重要意义。

随着比特币等数字货币的发展，出现越来越多的数字资产被盗事件。2011 年 6 月，一名名叫 AllinVain 的黑客获得一个矿场的硬盘，将两万五千个比特币转移到外部钱包。2014 年 2 月，交易所 Mt.Gox 被盗 85 万个比特币，损失约 4.67 亿美元，Mt.Gox 最终因存款到期无法兑现而宣布倒闭。2018 年 1 月，日本交易所 Coincheck 被盗 5 亿枚 NEM 代币，损失为 5.3 亿美元。2019 年 7 月，日本持牌加密货币交易所 BITPoint Japan 被攻击，损失达 35 亿日元（约 2.23 亿元人民币），2020 年 10 月，硬件钱包制造商 Trezors 遭到钓鱼攻击，用户资金大量流失。数字货币被盗事件远不止这些，从这些被盗事件中可以发现，大部分资产被盗发生在数字货币交易所，一些黑客经常关注交易平台的漏洞，交易所如果被攻击，很容易造成交易的资产流失。

（3） 数字钱包的发展

除了交易所外，用户还可以通过数字钱包进行数字资产交易。数字钱包是一种存储、管理和使用数字资产和密钥的工具。利用非对称加密算法形成的一系列密钥对就是存储在数字钱包中，每一个密钥对与用户的每一笔资产相关联，通过密钥对可以完成对数字资产的接收、转移及查询等功能。因此，数字钱包作为用

户使用数字资产的接口，在整个数字货币系统中起着至关重要的作用。并且由于资产存储、交易需求逐渐增加，数字钱包适用范围越来越广。

目前主流的数字钱包包括 Bitcoin core、imToken、Mist 等。据数字资产评级机构 TokenInsight 对全球数字钱包用户的统计，截止 2021 年 1 月，全球数字钱包用户在 2021 年第一季度，达到 6400 万 [11]。

除了市场上出现各种各样的数字钱包外，学术界也提出了很多数字钱包方案。按照私钥存储位置进行分类，可以将钱包方案分为软硬件钱包和托管钱包。按照签名方式，可以将钱包分为单签名、多重签名钱包和门限签名钱包。不同的数字钱包方案，使用的加密算法、签名方式以及私钥存储位置等不尽相同，钱包的安全性能也有所差异。例如软件钱包中用户私钥存储在本地数据库，当用户发起交易时，需要在联网的情况下使用私钥对交易进行签名，用户输入私钥等隐私信息时存在安全隐患，容易遭受钓鱼攻击，黑客很容易通过远程攻击的形式获取本地数据库中的用户私钥。硬件钱包虽然是在没有网络的情况下对交易进行签名，但是如果钱包丢失，可以通过暴力破解的方式获取其中的密钥。托管钱包因为将私钥交给第三方保管，存在内部人员攻击，第三方可以携款潜逃，而且所有私钥集中存储在第三方的服务器上，服务器容易成为攻击点，被黑客攻击。按照签名方式的不同，单签名钱包也存在单点威胁的问题；多重签名虽然有多个用户共同控制一个账户，抵御单点攻击，但是由于多重签名的公共地址是多个持有人的私钥共同生成的，公共地址与签名者的私钥存在关联性，黑客可以通过大数据分析手段获得签名者的私钥，对签名者的资产造成威胁；门限钱包同样采用多个持有者共同管理账户的方式，但是其采用分布式签名，公共密钥并不与签名者的私钥相关联，不会泄露签名者的隐私信息。

门限钱包方案采用 Shamir 秘密共享方案，由多个节点共同管理私钥。在（t，n）Shamir 秘密共享方案中，将秘密分割成份发送给 n 个节点，只有不少于个 t 节点合作才能重构秘密。

因此，基于以上研究背景，本文对区块链数字钱包的安全性以及数字签名方案进行研究。首先基于区块链的数字钱包进行安全性分析，按照私钥存储位置和私钥使用方式将数字钱包分成 6 类，对它们的安全性进行比较，然后从系统安全、数据安全两个方面进行安全性分析。其次针对门限钱包既能保障隐私又能抵抗单点故障问题，结合椭圆曲线数字签名算法，设计一种适用于数字钱包的门限椭圆曲线数字签名方案，提高数字钱包私钥存储及使用的安全性。

1.1.2 研究意义

（1） 理论意义

第一，对区块链数字钱包进行了安全性分析，为以后研究者研究数字钱包安全性提供参考思路。在现有关于数字钱包的文献中，很少有关于数字钱包安全性的研究，更多的是研究数字钱包的发展现状、钱包方案设计等方面。本文从安全性出发，研究影响数字钱包安全性的因素，并对这些因素进行总结。

第二，提出一种数字签名方案。当前门限签名技术处于发展阶段，由于算法复杂比较高，很少有研究者将门限签名应用在数字钱包中。本文将门限秘密共享方案与椭圆曲线数字签名算法相结合，提出了一种门限椭圆曲线数字签名方案。

（2） 实践意义

第一，对数字钱包了安全性分析，总结影响安全性的因素作为安全性指标，在实际中可以使用这些安全指标判断任何一种数字钱包的安全程度，并且使用这些指标可以不同的数字钱包方案的安全性进行对比分析。

第二，提出的门限椭圆曲线数字签名方案可用于数字钱包的设计中。首先在整个过程中多次加入反馈机制，降低参与者合谋的可能性，并且能够保证生成的公共密钥的安全性；其次，方案中的 ECDSA 算法是在经典 ECDSA 算法上进行改进，将生成签名和验证数字签名过程中的逆运算换成加法运算，在确保改进后的 ECDSA 保证安全性的前提下，降低算法复杂度，提高签名效率；最后方案引入同态加密算法，在不泄露个人隐私的情况下实现秘密碎片的共享，最后生成数字签名，使用同态加密算法提高了数据传输的安全性。提出的门限椭圆曲线数字签名方案能够抵抗合谋攻击，还能解决单点故障问题，可以适用于数字钱包方案中。

1.2 研究内容与创新点

1.2.1 研究内容

主要的研究内容为：

（1）研究数字钱包的安全性。以数字钱包的安全为研究对象，对数字钱包的安全性进行全面的分析，从不同的角度描述数字钱包可能存在的安全问题，例

如数字钱包的载体安全性、钱包存在哪些安全攻击以及钱包中保障数据安全的机制等。

（2）研究数字签名方案。传统的数字钱包方案中，私钥存储在单个位置，攻击者可以发起单点攻击，威胁数字钱包的安全。因此提出使用多重签名、门限签名等方法，提高私钥的安全性。由于多重签名需要签名者对交易信息逐个签名，交易效率低，而且可能暴露签名者的相关信息。因此针对单点故障和隐私泄露问题，本文选用门限签名方案。现有的门限签名方案基本上是与非对称加密算法相结合，例如 DSA 加密算法、ELGamal 加密算法和 ECDSA 算法，利用这些算法本身的数学难题，提高签名的安全性。由于数字货币系统生成的是 ECDSA 密钥对，因此本文提出一种门限 ECDSA 方案。该方案中不存在可信第三方，所有参与者通过相互通信传递信息，形成共享密钥和共享签名，在通信过程中，为了保证参与方传递信息的真实性，论文使用可验证方法，对参与者传递信息的准确性进行验证，从而保证对交易信息加密和签名过程的安全性。在进行签名阶段，还引入同态加密算法，保证签名着传输签名碎片的过程中不泄露自己密钥信息，保证数据传输过程中的安全性。

（3）研究门限椭圆曲线数字签名方案安全性和性能表现。通过理论分析和实验设计来评估本文所提出的门限椭圆曲线数字签名方案。在理论分析方面，从正确性、计算安全性、鲁棒性和匿名性四个方面分析提出的门限椭圆曲线数字签名方案，验证方案是安全的。在实验设计方面，通过算法生成共享密钥、生成共享签名和验证签名三个阶段判断算法复杂度和时间复杂度，并且对这三个阶段的算法复杂度与其他方案进行对比分析，证明提出的方案在保证安全的前提下还能降低算法复杂度，提高签名效率。

1.2.2 研究创新点

本文研究基于区块链的数字钱包的安全性以及密钥管理安全方案，具体创新点为：

（1）系统性分析了数字钱包的安全性分析。从系统安全、数据安全两个方面，分析影响数字钱包安全性的因素，通过这两个角度，我们可以评判一个数字钱包或者数字钱包方案的安全程度，为以后研究数字钱包安全性提供参考思路。

（2）提出一种新的数字签名方案。在传统的数字钱包方案中，私钥一般存储在本地数据库或者第三方服务器上并且存储位置比较单一，容易造成单点故障问题。为了提高数字钱包方案的安全性，本文提出一种门限椭圆曲线数字签名方

案，包括生成密钥、生成数字签名以及验证签名三个阶段。在生成密钥阶段，加入反馈机制，保证密钥分发和恢复过程的安全性。在数字签名阶段，引入同态加密，构造新的运算规则，实现在无中心的情况下，生成数字签名。通过新的数字签名方案，能够确保密钥的安全以及得到正确的数字签名。

1.3 研究方法

为增强研究成果在理论上的科学性及实践应用中的可操作性，本文坚持理论联系实际相结合原则，主要采用了理论研究法、实验设计法对基于区块链的数字钱包的安全性分析与密钥管理安全方案研究。

1.3.1 理论研究法

理论研究法是指根据特定研究问题，展开对理论基础知识的研究。为了提出一种比较全面的安全性分析和设计一种数字钱包密钥管理方法，需要相关的基础知识提供理论支撑。首先，在数字钱包安全性分析中，需要阅读并整理文献，对文献中关于数字钱包的安全性进行归纳总结，凝练出评判数字钱包安全的参考指标。其次，在设计新的门限椭圆曲线数字签名方案中，使用非对称加密机制和门限秘密共享技术相结合，为保证参与者在通信时的安全性，使用同态加密、安全多方计算等技术。

1.3.2 实验设计法

实验设计法是通过制定实验方法，验证可行性和有效性。本文拟用实验设计的方法，对提出的门限 ECDSA 方案进行实验分析和性能测试评估。

1.4 文章组织结构

本文共有 5 章，组织结构如下：

第一章，绪论。首先阐述论文的研究背景和研究意义，介绍了区块链技术、数字货币以及数字钱包的发展现状，表明研究本课题的必要性，然后简要概括论文的主要工作、研究创新点以及研究方法，最后对文章组织结构进行阐述。

第二章，文献综述。对当前数字钱包方案、影响数字钱包安全性因素以及门限 ECDSA 方案三个方面的研究现状进行阐述，分析当前方案中存在的问题，为后面的研究工作奠定基础。并且对当前的数字钱包按照私钥存储位置和私钥使用

方式进行分类，分析每种数字钱包的特点。最后为所提出的门限椭圆曲线数字签名方案提供理论技术基础，包括 ECDSA 算法、Shamir 秘密共享方案以及同态加密算法。

第三章，数字钱包安全性分析。首先从数字钱包种类出发，分析各种分类钱包的特点及安全性。根据安全性，分析影响数字钱包安全性的两个因素系统安全和数据安全。在系统安全方面，介绍几种威胁系统安全的攻击方式，总结攻击方式的实施难度和成本。在数据方面，研究运用在数字钱包中数据安全保护机制，并进行对比分析他们的性能。

第四章，提出一种数字签名方案。结合文章的研究背景，提高数字钱包数据安全性和避免单点故障问题，将门限技术与椭圆曲线数字签名算法相结合，设计一种门限椭圆曲线数字签名方案。首先详细描述生成密钥、生成数字签名和验证数字签名的过程，然后从理论上证明方案的安全性，最后对方案进行实验评估。

第五章，结论与展望。对论文的研究结论进行概括总结，讨论研究工作中存在的不足，最后对研究课题后续工作进行展望。

2 文献综述

随着比特币等数字货币的发展，数字货币和钱包的安全性变得越来越重要。学者们在研究数字钱包时，通常会针对钱包中某一个安全问题提出新的数字钱包方案，然后证明提出的数字钱包方案能够解决这一安全问题。由于一些钱包方案针对特定安全问题提出的，钱包方案之间很难进行安全性比较。因此本章首先阐述国内外有关数字钱包方案进行概述，按照私钥存储位置和私钥使用方式将数字钱包分为 6 大类，并详细介绍每种数字钱包。其次对影响数字钱包安全性的因素进行概括，包括系统安全和数据存储安全。最后，针对数字钱包方案中的单点故障问题，可通过多重签名和门限签名的方法解决，了解现有的门限签名方案以及存在的问题，确定将门限共享方案和 ECDSA 算法相结合是可行的，并对相关技术进行论述。

2.1 基于区块链的数字钱包方案

2.1.1 相关研究论述

数字钱包是用来存储和管理密钥对的工具，每个数字钱包包含一系列的密钥对和地址，并且密钥对和地址一一对应。市场上出现各种各样的数字钱包，例如比特币钱包、以太坊钱包等。学术界对基于区块链的数字钱包的研究主要还是从用户私钥着手，设计一种如何安全生成、存储以及使用私钥的钱包。文献[12]对私钥生成提出了一种改进的方案。该文献将随机种子和口令连接起来生成私钥，要想得到完整的私钥，随机种子和口令缺一不可，用户在本地存储随机种子而不是私钥，这样能保证用户私钥的安全性。文献[13]提出了一种基于 TrustZone 的联盟链安全轻钱包。该文献使用 TEE 和 SPV 机制，将用户的私钥等关键信息进行安全存储，提高了交易性能，并且解决了通过使恶意交易验证成功造成用户资产损失的问题。文献[14]提出了一种用于多个离线比特币交易的分层确定性钱包 MOBT。该文献利用分层确定性钱包的主公钥属性生成 MOBT 钱包的密钥对，用户只需要将比特币一次性存入钱包，从而减少了多个离线比特币交易时钱包的密钥存储空间，提高交易效率。文献[15]提出了一种硬件钱包 BlueWallet。该文献使用蓝牙低能量通信，能够安全签署比特币交易，并且 BlueWallet 使用 POS 机与区块链进行交互。文献[16-20]提出了各种门限钱包方案，门限钱包就是将密钥分成几个部分分别由几个参与者进行保管，只有达到一定数量的参与者才能重构

密钥。这几个文献就是针对门限签名算法中存在的问题进行改进和优化，文献[16]提出了秘密保护秘密分享的线上门限方案，防止参与者存在欺骗行为，保证钱包的安全。文献[21-22]提出了多重签名钱包，这是保证私钥使用过程安全而设计的一种钱包方案。在比特币多重签名交易过程中，只有达到所需签名数量交易才有效，利用多重签名算法，确保交易安全。

上述文献中提出各种各样的数字钱包方案，但是这些钱包方案不能代表所有的数字钱包。因此，本文按照私钥存储位置和私钥使用方式两个方面，将现有的数字钱包分为 6 大类，具体如图 2-1 所示，并且在第 2.1.2 节中详细介绍这 6 大类数字钱包。

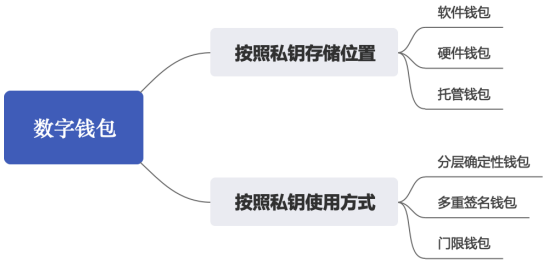

图 2-1 数字钱包分类

2.1.2 数字钱包分类

（1） 按照私钥存储位置分类

在现有的数字钱包中，用户私钥存储的位置主要有：存储于软件、硬件和可信第三方，对应的钱包就是软件钱包、硬件钱包和托管钱包。下面对这三种钱包运行原理进行介绍。

1） 软件钱包

软件钱包，顾名思义，是一个计算机程序的设备，通过这个程序实现与区块链交互，实现发送、接收交易，查看交易记录等功能。在软件钱包中，私钥存储在本地文件中，当用户使用私钥时，只需要访问存储私钥的文件即可。如图 2-2 所示。

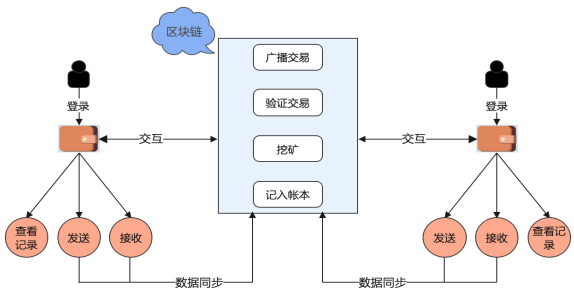

图 2-2 软件钱包与区块链交互过程

软件钱包按照是否需要下载完整的区块链和是否进行完整的交易验证，将钱包分为全节点钱包和轻节点钱包。全节点钱包在安装完钱包后，需要下载完整的区块链数据文件，数据同步后钱包才能正常使用。轻钱包也称为 SPV 钱包，使用简单支付验证机制，在不下载区块链完整数据的情况下验证交易。

2） 硬件钱包

硬件钱包将私钥存储在物理硬件中，私钥在生成、存储和使用过程中不接触到网络，杜绝私钥受到网络攻击。硬件钱包需要与联网设备连接后，才能实现与区块链的交互，如图 2- 3 所示。具体过程如下：

Step1：钱包初始化。设置 PIN 码，确保设备不会被未授权用户访问；生成私钥，完成后显示助记词，将助记词备份到卡片上，完成钱包初始化。

Step2：连接联网设备。钱包通过数据传输与联网设备连接，将钱包的地址信息发送出去、接收未签名的交易进行签名等功能。当前主要的数据传输方式有三种，分别是 USB、蓝牙和二维码，其中学术界研究的硬件钱包方案中主要的 USB 和蓝牙。这里的联网设备指的是能与区块链交互的设备，可以是电脑浏览器、客户端，移动客户端，POS 机等。

Step3：联网设备与区块链进行交互。联网设备收到签名后的交易，将其广播到区块链网络中，然后验证并打包区块，经过挖矿，将区块添加到区块链上，交易完成。

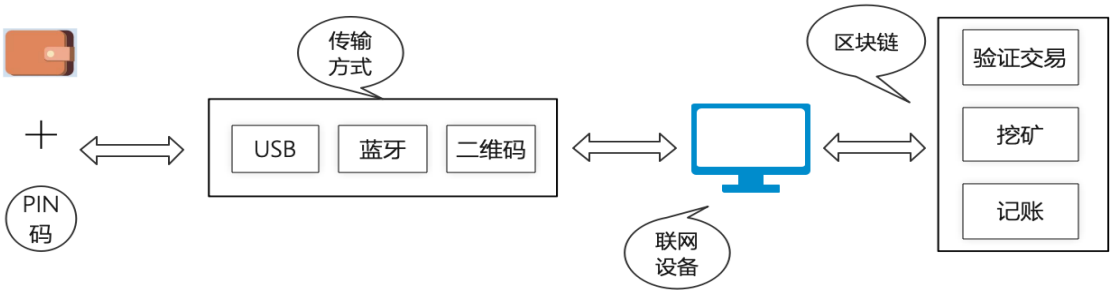

图 2- 3 硬件钱包与区块链交互过程

3） 托管钱包

为了保证数字资产的安全，用户将资产和密钥交给可信第三方保管，当用户需要交易时将指令发给第三方，由第三方执行与区块链交互，完成交易操作，这种钱包称为托管钱包。托管钱包十分便利，托管账户之间交易速度快、手续费低；用户存储在第三方的资产可以随时取出，而且不用担心忘记私钥或者助记词而失去资产，这样使得用户因个人原因忘记私钥或者操作失误导致资产损失的风险大

大降低。图 2-4 为托管钱包与区块链交互过程。

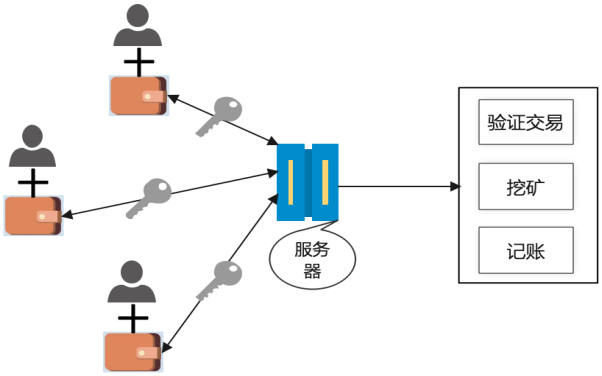

图 2-4 托管钱包与区块链交互

（2） 按照私钥使用方式分类

上述几种钱包方案是按照私钥存储位置进行分类。在区块链系统中，不仅私钥存储很重要，私钥的使用和管理也不容忽视。下面就按照私钥使用方式将钱包分成三类，分别是分层确定性钱包、多重签名钱包和门限钱包。

1） 分层确定性钱包

据统计，截止 2021 年 5 月，比特币系统已经产生了 6.4 亿笔交易，每个区块平均产生 2000 笔左右的交易。在 Bitcoin Core 钱包中，每产生一笔交易就会生成一对密钥对和一个地址，而且使用时需要给私钥备份，一旦丢失将会造成资产损失，所以如何管理私钥成了一大难题。分成确定性钱包（Hierarchial Deterministic Wallet，简称 HD 钱包）可以解决这一问题。HD 钱包是从一个种子生成一个树状结构存储多组密钥对，通俗的说就是通过种子生成一个主私钥，然后派生海量的子私钥和子公钥。HD 钱包是由 BIP32、BIP39 和 BIP44 共同定义的，其中 BIP32 描述了 HD 钱包如何派生密钥的过程，如图 2-5 所示。

2） 多重签名钱包

在比特币系统中，多重签名交易就是多个用户对一笔交易签名后交易，交易背后的资产由这些用户共同支配和管理。例如 n/m 多重签名交易指的是 n 个持有人中有 m 个同意交易并签名，则交易生效。如果钱包使用多重签名技术，用户想要发起一笔交易，交易需要有多个人的私钥签名才有效。多重签名钱包需要交易时，提前约定好所需签名数量、交易金额等事项，然后用持有人的公钥生成公共地址，一旦签名数量达到约定数量，交易生效并全网广播。具体交易生成过程如图 2-6 所示。

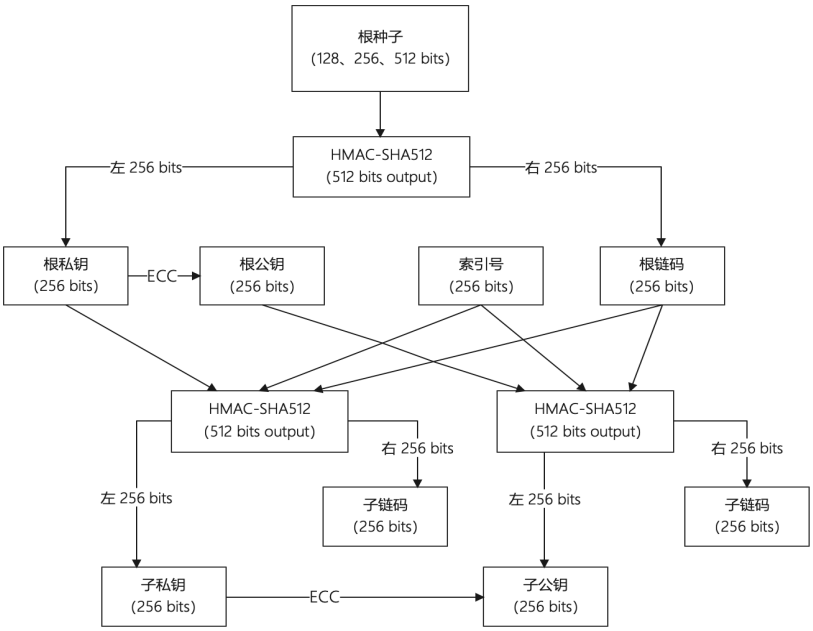

图 2-5 HD 钱包派生密钥过程

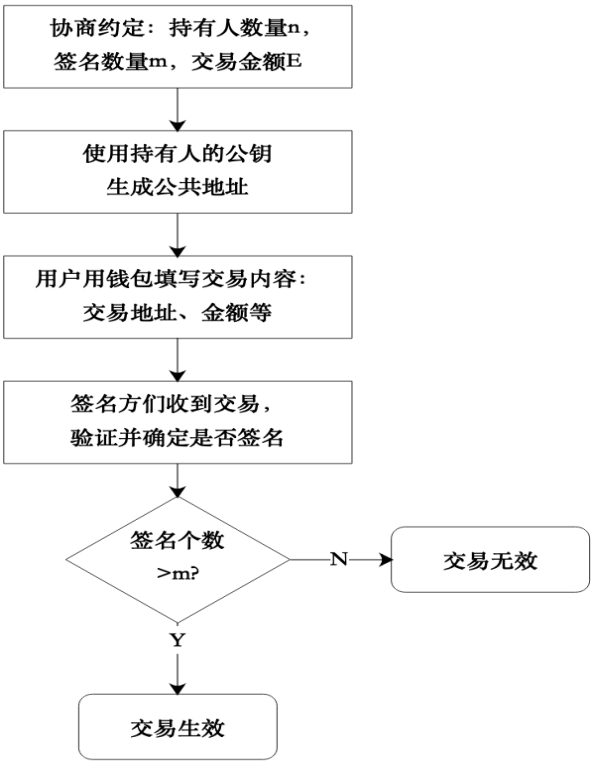

图 2-6 多重签名交易生效过程

3） 门限钱包

门限钱包一种使用门限密码学、安全多方计算等技术的钱包。门限密码学是秘密共享和密码学的结合。秘密共享最早是在 1979 年由 Shamir 和 Blakley 提出的，分别给出了两种秘密分享方案[23-24]。其中 Shamir 给出的是基于朗格朗日插

值法的秘密分享方案。真正出现门限密码学概念是由 Desmet 提出的，他认为门限密码学是秘密共享和密码学的结合。

林璟锵等人[25]设计了一种 SM2 椭圆曲线门限密码算法，介绍了 SM2 门限签名方案、SM2 门限交换协议方案和 SM2 门限解密方案，并通过安全性和效率分析，得出这三个门限方案在窃听攻击中不可伪造和健壮的，并且通信量和计算量相对于其他算法而言较小，效率高。下面给出在无可信中心情况下 SM2 椭圆曲线门限密码算法的密钥生成、门限签名和门限解密三个过程，以（2，3）门限密码为例。

密钥生成过程：3 个参与方分别生成自己的私钥s，然后使用 Shamir 秘密分享将自己的私钥中s_i份额分给其他两个参与者；参与者通过获得其他参与者的私钥份额，通过私钥份额计算公钥份额并全网广播；参与者通过广播中的公钥份额计算中公钥。

门限签名过程：当一个参与者发起交易，将未签名的交易单发给其他两个参与者，参与者对交易进行验证，然后可以选择用自己的私钥给交易进行签名并广播，如果三个参与者里至少有两个签名，那么用户可以合并签名生成 SM2 签名，交易生效。

门限解密过程：当收到密文后，如果至少有两个参与者用自己的私钥进行解密并广播，那么就可以使用拉格朗日插值公式计算出全部明文。

门限钱包方案不仅能抵抗单点故障问题，还可以决解多节点效率低等问题。但是它还是存在一些安全问题。门限技术使用安全多方计算，引入多个参与方，那么就可能存在参与方共谋的问题，一旦恶意参与方共谋数量达到门限值，账户资产的所有权将被他们所控制，提高账户资产流失的风险。

2.2 区块链数字钱包安全性分析

目前，数字货币攻击事件频繁发生，给数字货币服务商及用户造成了巨大的经济损失，因此数字货币的安全问题受到广泛的关注。数字钱包，作为数字货币存储设备，其安全问题也不容忽视。通过大量阅读文献后，发现现有的关于数字钱包的文献中，更多的是研究一种数字钱包方案的设计，然后在方案设计后对方案的安全性进行分析，例如分析钱包方案存在的安全攻击，数字钱包的隐私安全、访问安全等，而单独对数字钱包的安全性进行分析的文献极少。通过阅读整理文献，从系统安全和数据安全两个方面分析数字钱包安全性。

2.2.1 系统安全

本文研究的是基于区块链的数字钱包，因此考虑的系统安全是数字货币区块链系统的安全漏洞和攻击事件。武勇等人[26]以区块链技术为研究对象，提出了一种四层技术体系，包括网络与存储层、数据与算法层、共识与合约层和应用支撑层，各层之间相互支撑，详细描述区块链核心组件。提出四层体系后，根据每层的技术特点，对区块链存在的安全风险进行分析。魏松杰等人[27]研究区块链公链应用的安全问题，以比特币系统和以太坊系统为代表，研究加密数字货币应用的区块链系统中存在的各种安全威胁，提出了 36 种安全攻击，通过区块链系统架构对其进行分类，并针对分类提出可行技术线路和防御方法。刘九良等人[28]对区块链安全进行研究概述，其中包括系统安全研究，提出系统安全主要包括共识算法安全、加密算法安全、智能合约安全和系统资源安全，然后详细分析这四个部分存在的技术漏洞以及存在的安全攻击。苟俊卿等人[29]对 Libra 区块链系统进行了安全性分析，主要从分布式网络、共识机制、密码算法和智能合约四个角度，分析 Libra 系统中存在的安全风险，然后总结现有的 Libra 区块链安全检测技术，最后提出一种 Libra 区块链安全态势感知平台，通过这个平台可以实现对区块链出现的一些异常行为例如内部异常、智能合约异常等进行监控和预警。

2.2.2 数据安全

目前在区块链系统中，数据安全管理逐渐受到人们的关注，如何安全存储数据、保护隐私数据等已经成为当前的研究热点之一。毕晓冰[30]设计一种基于 iOS 系统的区块链数字钱包，利用 Keychain 安全存储机制改进私钥存储，实现私钥离线自由、安全存储；同时引入 SPV 技术，节点只需要在链外备份存储数据，减少节点内存存储负担；最后还采用 Realm 持久化存储方案，提高了交易信息的安全性。梁秀波等人[31]对区块链数据安全以及隐私保护技术进行研究，从数据存储安全、数据隐私安全等四个方面总结当前区块链系统中存在的安全问题以及解决措施。Zerocoin 引入零知识证明的方法保护用户交易数据，基于双重离散对数的方式对交易的来源进行匿名，在交易付款时保护付款方的信息[32]。 Dash 是基于比特币技术的数字货币，交易双方需要使用固定的数值来进行混币交易，其中有中介节点负责打乱输出地址[33]。 Dash 虽然设置了许多负责混币措施的中介节点来降低地址间的关联性，但是 Dash 要求中介节点抵押高昂的担保金来防止中介节点作恶。门罗币（Monero）是利用环签名技术实现混币机制的数字货币，与

其他混币机制相比，在进行混币的过程中，任意 Monero 混币用户可以自行实现混币过程，无须与其他混币用户进行交流，这样可以避免其他混币用户泄露混币过程的风险[34]。

2.3 门限椭圆曲线数字签名方案

2.3.1 相关研究论述

目前，门限椭圆曲线数字签名方案按照是否有可信中心可分为两类，一类是有可信中心，由可信中心集中生成私钥和签名；另一类是无可信中心，所有节点相互通信，通过安全多方计算等技术生成私钥和签名。Desmedt 等人设计了门限签名方案，该方案使用了门限秘密共享算法和 RSA 数字签名算法[35]。2004 年 Tzer-Shyong 等人提出了将密钥特征与门限共享方法相结合，提出了一种数字签名方案，由于该方案不能进行身份追踪和交易撤销，实用性不高[36]。文献[37]对 Tzer-Shyong 提出的签名方案中的密钥生成方式进行改进，使得合谋攻击的难度值等价于椭圆曲线离散对数难度值。文献[38]基于双线性映射和秘密共享思想提出了一种基于身份秘密的门限签名方案，采用基于身份的(t,t)秘密共享算法，提升了算法的执行效率。文献[39]提出了一种离散对数难度的门限签名方案，能够有效抵抗针对秘密共享技术的攻击手段。Goldfeder 等人提出利用门限签名技术实现比特币密钥的多方控制功能，利用门限密码学技术实现密钥的可信管理[40]。Asmuth 等人使用中国剩余定理提出了一种门限秘密共享方案 Asmuth-Bloom，该方案于基于 Shamir 秘密共享技术相比，计算量较小，但是由于该方案是在不安全的通信信道中传输数据，因此不能保证数据的安全性[41]。文献[42]在文献[41]的基础上提出了一种使用 ElGamal 算法与 Asmuth-Bloom 门限秘密共享相结合的方案，能够防止秘密份额在传播过程中被篡改。文献[43-44]提出了基于门限 ESCDA 系统，t 个参与者重构密钥，但却需要 2t+1 个参与者才能签名。文献[42]提出一种无中心的门限椭圆曲线数字签名方案，该方案实现了多节点控制钱包私钥，但是该方案不能抵抗伪造性，不能防止出现不诚实参与者的情况。文献[45]提出了一种可验证的门限椭圆曲线数字签名方案，能够验证是否存在不诚实玩家，但是该方案有可信中心，有可信中心最终生成共享私钥和共享签名。文献[46]和[47]都提出了一种无信任中心、可验证的门限 ESCDA 方案，其中文献[46]使用同态加密算法实现多方之间的签名，文献[47]使用非交互的零知识证明协议，在不

泄露个人隐私的情况下生成共享私钥。

在上述阐述的门限签名方案中，主要都是使用加密算法和门限共享方案相结合。使用的加密算法主要有非对称加密算法，例如 DSA 算法、ElGamal 加密算法和椭圆曲线数字签名算法，基于这些算法本身的数学难度问题，保证签名方案私钥的安全。使用的门限秘密共享方案主要包括两种，Shamir 秘密共享方案和基于中国剩余定理的秘密共享方案，前者安全性更高，后者计算量小，复杂程度低。并且，大多数是无中心门限签名方案或者可验证门限签名方案，很少有同时具备无中心和可验证的门限签名方案。即使同时具备这两个特点的门限签名方案，也不能保证签名方案中密钥的安全性。因此，本文将 shamir 秘密共享方案与椭圆曲线数字签名算法相结合，设计一种无中心、可验证且安全性高的门限椭圆曲线数字签名方案。下面对方案中所涉及到的相关知识进行详细介绍，其中包括 Shamir 秘密共享方案、椭圆曲线数字签名算法以及同态加密算法。

2.3.2 相关技术论述

（1）Shamir 秘密共享方案

(t,n)Shamir 秘密共享是将一个秘密分割成 n 个部分并交给 n 个参与者保管，其中 t 个及以上的参与者能够重构秘密，少于 t 个参与者不能重构秘密。具体过程如下：

（1） 初始化。n 个参与者C_1、C_2、…、C_n，秘密为σ，随机选取大素数q，随机生成多项式$f(x)=a_0+a_1x+\cdots+a_{t-1}x^{t-1}(mod\ q)$，其中$\sigma=a_0$。

（2） 分割秘密。计算$\sigma_i=f(i),i=1,2,\cdots,n,$ 把σ_i作为秘密份额发送给参与者C_1、C_2、…、C_n；

（3） 重构秘密。任意选取其中的 t 个参与者，不失一般性，选择C_1、C_2、…、C_t，使用其秘密份额σ_i，利用拉格朗日插值公式重构秘密σ，即

$$\sigma=f(0)=\sum_{i=1}^{t}\sigma_i\prod_{j=1,j\neq i}^{t}\frac{-c_j}{c_i-c_j}(mod\ q)。$$

（2）椭圆曲线数字签名算法

椭圆曲线密码体制（ECC，Elliptic Curve Encryption），可以应用在不同的场景并涉及到不同的算法。当 ECC 生成和验证数字签名时，使用椭圆曲线数字签名算法（ESCDA ，Elliptic Curve Digital Signature Algorithm）。下面给出 ECDSA 算法的具体过程。

1) 生成签名

（i）在有限域F_p上随机选择一条椭圆曲线$E_p(a,b)$,G是E的生成元，q是G的阶，其中p和q是两个很大的素数，M是需要签名的消息，$H(\cdot)$是哈希加密函数。

（ii）选取一个随机数$v \in Z_q^*$，计算$P = vG$，则v为私钥，P为公钥。

（iii）选取随机数$k \in Z_q^*$，计算$kG = (x_1, y_1)$、$r = x_1(mod\ q)$，如果$r = 0$，则返回第 2）步。

（iv）计算消息M的哈希摘要$m' = H(M)$，将m'转化为整数m。

（v）计算$s = k^{-1}(m + vr)(mod\ q)$，如果$s = 0$，则返回第 2）步。

（vi）输出签名(r, s)。

2) 验证签名

收到签名(r, s)后，对其有效性进行验证。已知消息M，公钥P，签名(r, s)。因为

$$(m + vr)G = mG + vrG = mG + Pr$$

若签名满足下列等式，则说明签名有效：

$$s^{-1}(mG + \mathrm{Pr}) = kG$$

（3）改进的椭圆曲线数字签名算法

文献[48]对 ECDSA 算法进行了改进，将在有限域F_p上的逆运算换成了加法运算，改进后的 ECDSA 算法的安全性和原来的相同，同时效率有所提高。改进前$s = k^{-1}(m + vr)(mod\ q)$，改进后$s = (k + mvr)(mod\ q)$，最后输出签名$(r, s)$。在验证签名的有效性时，若下面等式成立，则签名有效：

$$kG = (sG - mPr)(mod\ q)$$

（4）同态加密算法

同态加密算法是一种特殊的加密算法，在密文上运算等同于在明文上进行相应运算后再加密[49-50]。同态加密算法按照运算法则，可以划分为加法同态加密、乘法同态加密和全同态加密。前两种加密算法仅对于加法或乘法具有同态性，后一种加密算法对加法和乘法都具有同态性。全同态加密由于其算法的复杂性和安全性问题，还未进行实践和应用，而加法同态和乘法同态方案效率高，已经被运用在实际场景中，例如 Paillier 同态加密算法，应用在云计算中，保护隐私数据的安全。本文使用的就是 Paillier 同态加密算法E。

3 区块链数字钱包安全性分析

3.1 引言

近年来，数字钱包和交易所被攻击、数字资产被盗取的事件时有发生。基于区块链的数字货币还处于发展阶段，很多技术和机制还不完善，导致数字钱包仍有大量的隐患难以解决，面临着很多的安全风险。数字钱包存储管理密钥，是连接区块链系统与用户之间的桥梁，数字钱包的运行依赖于区块链系统。因此在研究数字钱包安全性时，需要考虑数字钱包背后的区块链系统的安全性。在上一章节中，按照私钥存储位置和私钥使用方式两个角度，将数字钱包分成了软件钱包等 6 类，从交互过程、交易特点等方面介绍了这 6 类数字钱包，但是并未对这 6 类数字钱包的安全性进行分析，因此，在本章节中，首先对 6 类数字钱包的安全性进行比较。然后，从区块链安全性开展研究，研究当前区块链系统中存在的安全攻击，以及在区块链系统上确保交易数据安全性的机制。

3.2 不同种类数字钱包的安全性比较

按照分类，将钱包分为软硬件钱包、托管钱包、分层确定性钱包、多重签名钱包和门限钱包。通过这些钱包方案用户可以实现与区块链交互，完成转账、接收、查询、代币交易等功能，但是钱包方案落地还需要考虑其安全性，在开发过程中要进行安全性分析。

3.2.1 不同数字钱包安全性总结

软件钱包将私钥存储在本地数据库，使用私钥对交易签名需要在联网的情况下完成，用户在浏览器或者应用程序中直接输入私钥存在安全隐患。攻击者可以发起钓鱼攻击，远程监视用户交易设备，一旦用户输入私钥等隐私信息时，攻击者即可获得这些隐私信息。

硬件钱包将私钥存储在物理设备中，例如 USB。在硬件钱包中，私钥不直接接触网络，用户输入私钥进行签名是在没有连接网络的情况下完成，然后再进行其他操作，因此软件钱包的安全性高于软件钱包。但是，如果硬件钱包的载体丢失或者被窃取，攻击者可以通过暴力破解的方式获得密钥，例如 Trezor 硬件钱包

可以通过电压故障物理破解。

托管钱包将私钥存储在第三方服务器上，存在两个安全问题。第一，内部攻击。第三方如果不可信，用户将私钥存在服务器上，会让资产处于危险的状态，一旦第三方不守承诺或者直接窃取用户私钥，用户将会失去资产的所有权。第二，单点攻击。所有托管用户将自己的私钥存储在第三方的服务器上，服务器上会涌入大量的私钥，攻击者会发起攻击造成服务器瘫痪，一旦攻击成功，将会有大量的私钥丢失。

分层确定性钱包虽然只需存储备份主密钥和随机种子，但是由于其他密钥由主密钥派生的，密钥之间关联性高，攻击者可以通过子私钥和主公钥可以恢复主私钥，一旦拥有主私钥，用户所有资产的安全隐患非常大。

多重签名钱包使用多重签名的方式，共同管理账户里的资产，但是多重签名钱包存在安全问题。第一，可能会泄露账户隐私。因为多重签名的公共地址是由多个持有人的公钥共同生成的，如果攻击者使用暴力破解或者其他方法，是很容易知道账户是由哪些私钥控制，进而会泄露用户的一些隐私信息。第二，容易遭受 DOS 攻击。多重签名技术为了保证签名效率，有些签名算法要求签名者在规定时间内完成签名。攻击者可以发起拒绝服务攻击，使得系统无法正常提供服务，签名者无法在规定时间内完成签名交易。

门限钱包方案不仅能抵抗单点故障问题，还可以决解多节点效率低等问题。但是它还是存在一些安全问题。门限技术使用安全多方计算，引入多个参与方，那么就可能存在参与方共谋的问题，一旦恶意参与方共谋数量达到门限值，账户资产的所有权将被他们所控制，提高账户资产流失的风险。

3.2.2 不同数字钱包安全性比较

在私钥存储位置上，软件钱包、分层确定性钱包、多重签名钱包和门限钱包都是将私钥存储在本地数据库，需要联网设备才能与区块链交互，安全性低；托管钱包将私钥交给可信第三方保管，私钥的安全性取决于可信第三方，因此其安全具有不确定性；硬件钱包将私钥存储于物理硬件中，能够杜绝私钥接触网络，因此安全性比其他五类高。

在私钥使用方式上，软件钱包、硬件钱包和托管钱包都是通过单节点的方式进行使用，容易造成单节点故障；分层确定性钱包不需要备份私钥，而是通过备份的种子和根私钥生成新的密钥，安全性比前三类高；多重签名和门限钱包都是采用多节点的方式，但是多重签名钱包可以通过公共公钥获取一些隐私信息，安

全性程度低于门限钱包。通过表对 6 类数字钱包的优缺点、安全性进行总结，如表 3-1 所示。

在评估各类数字钱包的安全性时，从私钥存储位置和私钥使用方式两个方面考虑。在私钥存储位置，不联网的数字钱包的安全性高于联网的数字钱包；存放在第三方服务器上的私钥管理效率高于本地存放的数字钱包。在私钥使用方式时，单签名方式的安全性低于多签名的方式；将私钥集中存储在一个位置的风险高于由多个人共同管理私钥的风险。

表 3-1 各类数字钱包安全性比较

类型	优点	缺点	安全性	
			私钥存储位置	私钥使用方式
软件钱包	易安装，交易效率高	连接网络，安全性低，私钥管理难度高	低	低
硬件钱包	私钥与联网设备隔离，增强私钥安全性	便携度低，不易管理私钥	高	低
托管钱包	引入可信第三方，高效管理私钥	容易存在不可信第三方；出现内部攻击	中	低
分层确定性钱包	减少私钥备份，降低私钥管理难度，节约内存空间	根密钥和子密钥关联度高	低	中
多重签名钱包	多节点管理私钥，降低单点风险	需要较高的算力、交易效率低，可能出现合谋攻击	低	中
门限钱包	抵抗单点攻击，交易效率高	算法复杂度高，可能出现合谋攻击	低	高

3.3 系统安全

基于区块链的数字钱包底层采用区块链技术，但是目前的区块链技术还未十分成熟，区块链系统中仍然存在一些安全漏洞，攻击者们借助这些安全漏洞对系统发起安全攻击，一旦攻击成功，将会对区块链系统造成巨大伤害。区块链不稳定会影响数字钱包的安全，因此本文从区块链系统中存在的安全攻击出发，研究7种典型的安全攻击。

3.3.1 以比特币为代表的区块链系统的安全攻击

在比特币为代表的加密数字货币是区块链1.0时代，此时区块链系统实现数字货币间的交易，包括转账、代币交易等，主要发挥的是支付和价值存储的功能。在比特币中，由于共识机制的问题，有三种典型的攻击，分别是双花攻击、51%攻击和女巫攻击。接下来介绍这三种攻击的攻击原理，并提出防御方法。

（1）双花攻击

在比特币系统中，当系统中存在交易时，矿工节点争夺交易的记账权后进行广播给周围节点。由于全网矿工节点都在挖矿，可能存在两个矿工同时挖到矿，此时系统中所有节点都会收到两个区块高度相同的新区块，此时比特币会进行暂时的分叉。

双花攻击，又称为双重消费攻击，攻击者通过不停发起和撤销交易，用一定数额的比特币实现在多个账号间的转账从而获利。双花攻击能实现的原理就是利用上面提到的比特币会暂时的分叉，如图 3-1 所示。双花攻击的具体过程如下：

Step1: 作恶节点向 1 btc 向节点 M 发起一笔转账交易 A，交易 A 进入未确认交易池；

Step2: 同时作恶节点用 1 btc 向自己其他的账号地址 N 发起转账交易 B，交易 B 也进入交易池；

Step3: 此时矿工 Tom 和矿工 Bob 同时分别挖到包含交易 A 和交易 B 的区块，并进行广播给周围的节点，于是区块链发生了分叉；

Step4: 矿工 Tom 周围的节点先收到 Tom 打包的区块，于是用该区块延长自己的区块链，而矿工 Bob 周围的节点先收到 Bob 打包的区块，用该区块延长自己的区块链，此时整个系统中出现了两条主链；

Step5: 此时作恶节点采用各种手段，使得包含交易 B 的所在区块链更长，根据

区块链最长链的原则，包含交易 A 的所在链被废弃掉，但由于交易 A 之前已经被确认，所以交易有效，认为节点 M 收到了 1 btc，但是由于交易 B 所在链为主链，所以节点 M 并未收到 1 btc，实际是作恶节点的其他地址收到了 1 btc，因此攻击成功。

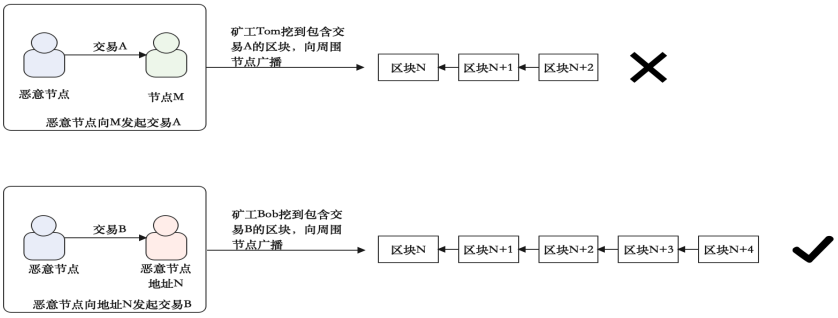

图 3-1 双花攻击原理

防御方法：在交易时设置一个承诺机制，承诺交易时不进行双花，如果出现双花，则公开该笔交易的私钥，其他成员就可以通过私钥找回货币，并对进行双花的节点进行惩罚。

（2） 51%攻击

在比特币系统中共识算法采用工作量证明机制（POW），用来证明矿工节点的工作量。矿工通过算力来达到自己的工作量，如果计算正确将获得区块的记账权。51%攻击是指作恶节点获得全网一半以上的算力，他就有较大优势获得区块的记账权，作恶节点就可以修改账本或者阻止其他人挖矿，从而威胁到整个区块链的系统安全。

作恶节点通过 51%攻击主要有两种目的，一种是修改区块链中的数据，一种是为了比特币奖励。修改区块链中的数据的方式和双花攻击原理相同，作恶节点使用一笔资金发起多币交易，然后利用一半以上的算力，使得对自己有利的一条区块链为主链，从而达到篡改数据的目的。51%攻击另外一种就是为了获得比特币奖励。具体原理为作恶节点利用 51%算力比其他节点更快挖到矿，但是选择延迟广播，然后继续在原来链上继续挖矿，等挖到足够多的矿后一起公布出来。在广播后，其打包到区块链的区块足够多，比其他的链长，根据区块链最长链的原则，作恶节点挖矿所在的链为主链，那他将获得连续区块的奖励。这种攻击也称为自私挖矿攻击。表 3-2 是挖出连续区块和算力的关系，可以看出当算力在 50%时，连续挖到 6 个区块的可能性约为 1.6%，是算力为 10%的节点的一万五千多倍。因此，如果一个节点的算力越大，挖矿的优势更大，挖到连续区块的可能性

更大，因此能获得更多的奖励。

表 3-2 算力与连续区块的关系

p \ n	1	2	3	4	5	6
0.1	0.1	0.01	0.001	0.0001	0.00001	0.000001
0.3	0.3	0.09	0.027	0.0081	0.00243	0.000729
0.5	0.5	0.25	0.125	0.0625	0.03125	0.015625

防御方法：在比特币系统中只要采用 POW 共识机制，就可能出现算力过度集中的可能性，因此不能完全避免 51%攻击。但是，可以采用一些激励机制，抵制算力中心化。

（3） 女巫攻击

在 P2P 网络中，为了解决来自恶意节点的安全威胁，通常会引入冗余备份机制，将数据备份到多个节点或者将数据分割存储在多个节点上。正常情况下，一个设备代表一个节点，该节点用特殊的 ID 来标识。但是如果系统中缺少身份认证机制，攻击者可以只需要一个设备，但是在网络中广播多个 ID 充当多个节点。在区块链系统中，有些区块链采用拜占庭容错机制作为共识机制，该机制达成共识的条件是：当网络中的恶意节点的个数不超过总节点的 1/3 时，认为全网络达成了正确的共识。

女巫攻击利用拜占庭共识机制，通过生成超过 1/3 的作恶节点，达成错误的共识以实现特定的目标。女巫攻击具体方式如下：假设作恶节点 P 构造不同的 ID 充当节点 P_1，P_2，…，P_{n+1}，网络中其他诚实节点为 S_1，S_2，…，S_{2n}。作恶节点 P 发起一笔交易，作恶节点 P_1，P_2，…，P_{n+1} 投赞成票，其他节点不管投赞成还是反对票，赞成的票数已经超过 1/3，则全网达成一致共识，该交易发起成功。如图 3-2 所示。

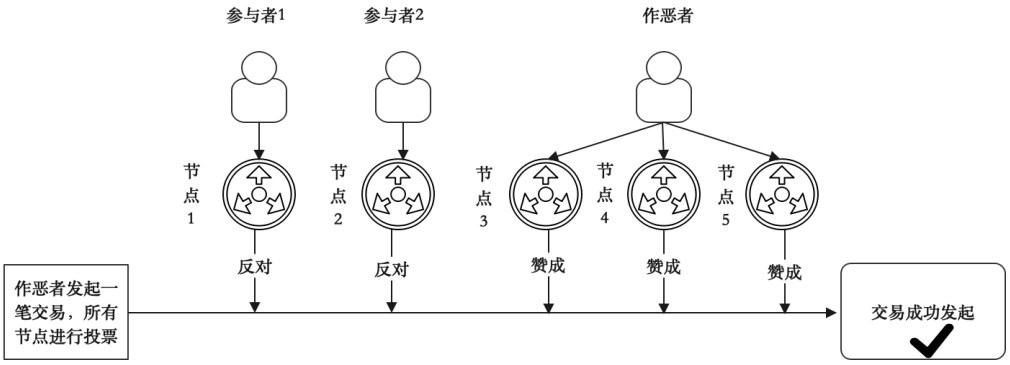

图 3-2 女巫攻击原理

防御方法：第一种加入身份验证机制，通过节点身份认证，阻止攻击者伪造

节点。第二种，如果节点需要参与交易投票需要交纳一定的费用，通过设置成本门槛，降低女巫攻击发生的可能性。

以上三种攻击是针对区块链系统的共识机制存在安全隐患而发起的攻击，区块链的共识机制除了 POW、拜占庭机制以外，还有 POS、DPOS、PoA 等共识机制，因此存在的安全攻击还包括像傀儡挖矿攻击、贿赂攻击、币龄累计攻击、无利害关系攻击、远距离攻击、削弱攻击等。

3.3.2 以以太坊为代表的区块链系统的安全攻击

区块链 1.0 指的是以比特币为代表的加密数字货币，则区块链 2.0 指的是以以太坊为代表的能够在区块链上运行智能合约的区块链系统，智能合约是区块链 2.0 的核心技术。在以太坊系统中，采用以太虚拟机作为智能合约的运行环境，具有图灵完备的特点。智能合约使得区块链系统具有较高的实用性和编程性，但是其在编写过程中仍然存在一些安全隐患，从而导致一些安全攻击。下面介绍智能合约中可能出现的 4 种攻击以及防御方法。

（1） 时间戳依赖攻击

在区块链中，时间戳是证明区块被打包的时间先后的一个有效证明，在以太坊系统中，大多数的智能合约执行条件包含时间戳，那么时间戳对智能合约的执行结果有影响。在以太坊系统中规定，矿工每处理一个新的区块时，新区块与前一个区块的时间戳的差小于 900s，则新的区块的时间戳是合法的。例如一个抽奖合约中，中奖编号与时间戳有关，是通过时间戳和其他变量计算出来的。作恶节点在挖矿时可以提前计算不同的时间戳的编号，设置中奖编号，然后把奖品送给这个编号的人。时间戳依赖攻击就是利用上面的原理，恶意节点可以将触发智能合约条件的时间戳设置成对自己有利的时间戳，从而达到自己的特定目标。

防御方法：在智能合约中不使用时间戳作为合约执行顺序的条件，可以选用区块编号作为改变合约状态的依据。

（2） 交易顺序依赖攻击

在区块链系统中，所有交易先放入到交易池中，然后按照一定的时间顺序确认并打包交易。在以太坊中，决定交易确认的时间顺序的因素是交易费（gas），交易发起者给的 gas 越高，交易被确认的越快，而智能合约的执行结果与交易处理顺序有关。例如，作恶节点发起一个解题的合约，在合约中给出较高的解题奖

励。当有人提交题目的正确答案后，由其他节点进行确认通过后，合约才能执行奖励。但是作恶节点在有人提交题目答案时，再次发起一个将奖励额度调低的交易，并给出比刚才的交易更高的交易费，那么验证节点在确认交易时会优先确认这一笔交易，最终导致答题者拿到较低的奖励，而作恶节点以一个较低的成本就买到了正确答案。

防御方法：可以通过提高交易的费用，降低攻击者重新发起新的交易的可能性。

（3） 可重入攻击

当一个智能合约调用另外一个智能合约时，通过修改回调函数的内容，使得两个智能合约循环被调用。可重入攻击最典型的案件就是“The DAO”事件。The DAO 得智能合约中有一个 splitDAO 函数，该函数进行一次合法调用后又出现再次调用自己，然后进入非法调用自己的循环。

防御方法：更新合约的余额状态，然后发送资金，同时加入验证机制，对合约中的 Gas 进行验证，如果出现重复调用时，拒绝执行。

（4） 调用深度攻击

在以太虚拟机中，会对智能合约的相互调用的深度设置一个阈值，一旦超过这个阈值，哪怕在逻辑上调用不存在任何错误，都被认为调用失败，不再进行调用。作恶节点可以通过控制调用深度的阈值，使得合约中的一些重要操作不被执行。

防御方法：加入验证机制，如果有成员多次调用智能合约，使智能合约的深度达到阈值附近，则将该成员剔除。

以上几种攻击都是基于智能合约存在的漏洞到导致的攻击，除了以上几种攻击意外，针对智能合约的攻击还包括整数溢出攻击、未处理异常攻击、逻辑漏洞攻击、平衡攻击等。

3.3.3 各种攻击的安全性总结

系统安全对整个区块链系统的安全起到了至关重要的作用，由于目前区块链技术还没完全成熟，区块链的架构设计中的一些设定导致一些安全隐患存在，攻击者们利用安全隐患和漏洞发起攻击，从而威胁整个区块链系统的安全。本节描述了在共识机制和智能合约中存在的攻击，表 3-3 对这些攻击进行总结。

在评估各类攻击的安全风险程度时，通过发起攻击的成本开销、可能需要花费的时间两个方面对发起攻击的实施难度进行判断。实施难度低意味着攻击基本不需要花费额外的成本或者时间，就可以完成攻击。例如女巫攻击，只需要攻击者构造多个节点身份作为伪装节点，公布到整个 P2P 网络中，破坏整个系统中的一些决策。时间戳依赖攻击和交易顺序依赖攻击，攻击者只需要在特定的时间点拦截交易，成功实现攻击。实施难度中等意味着攻击者需要花费一定的成本以及时间才能完成攻击。例如双花攻击，攻击者需要不断的发起和撤销交易，因此需要付出一定的交易费用。例如可重入攻击，攻击者需要发送一笔交易，导致合约账户一直重复执行直到合约账户的资源消耗完。例如调用深度攻击，攻击者需要了解智能合约的调用深度，通过花费一定的交易费用，才能实施攻击。实施难度高意味着攻击者需要投入大量的成本以及时间，才能完成攻击。例如 51%攻击，攻击者需要掌握全网 51%以上的算力，这需要花费大量的成本才可能实现。

表 3-3 安全攻击分类总结

攻击种类	应用系统	共识机制	实施难度	成本开销
双花攻击	比特币、以太坊等	不限	中	中
51%攻击	比特币等	POW	高	高
女巫攻击	比特币、以太坊等	BFT	低	低
时间戳依赖攻击	以太坊等	不限	低	低
交易顺序依赖攻击	以太坊等	不限	低	低
可重入攻击	以太坊等	不限	中	中
调用深度攻击	以太坊等	不限	中	中

3.4 数据安全

在早期的以比特币、以太坊为代表的区块链系统中，交易数据是公开透明的，所有的交易记录都可以在钱包等接口中查询。但是随着区块链技术被应用到其他各个领域中，例如金融、医疗等，由于有些行业的特殊性，交易记录中可能包含一些隐私数据，因此需要对这些隐私数据进行保密。另外，由于所有交易记录公开且可追溯，攻击者们可以使用大数据分析等手段，对交易数据中的资金流量、交易的输入输出地址等信息进行统计分析，发现不同交易之间的关联性，从而可能会获取交易者的账户信息甚至可能获得其真实身份，这将对用户的数据安全造成严重威胁。为了增强数据的安全性，研究者们提出各种解决方案，例如应用广

泛的混币机制，对数据进行加密的加密技术等。

3.4.1 基于混币机制的数据安全

混币机制的实质是对交易内容进行混淆，将多个交易混合在一起，使得交易的输入地址和输出地址的分离。通过这种方法，可以增加攻击者分析交易的难度，提高交易数据的安全性。根据是否有第三方节点，可以将混币机制分为中心化的混币机制和无中心化的混币机制。

（1） 中心化的混币机制

在中心化的混币机制中，需要进行混币的用户将资金发送给中心节点，由中心节点执行混币过程，将混币资金进行多次交易，然后将资金流向参与混币用户指定的接受者。通过这种方法，所有混币资金进行打乱再分配，攻击者很难同时知道一笔资金的流出和去向。但是混币过程中心化，很有可能存在内部攻击，中心节点收到混币资金后进行混币过程，而是占为己有。并且由中心节点混币，用户不能完全确定混币过程中有没有泄漏数据信息。因此针对这一问题，研究者们引入数据签名技术，根据数字签名不可伪造和不可抵赖等特点，增加中心节点的信任度。

Mixcoin 是一种中心化的混币机制，为用户提供混合服务，Mixcoin 为提高交易的匿名性，一般要求参与混币的用户提供相同的资金。为了解决上面问题，Mixcoin 加入承诺机制，中心化节点向参与混币的用户做出承诺，约定混淆金额、输入输出地址、时间等内容。图 3-3 为 Mixcoin 工作原理。如果中心化节点没有按照承诺中规定的时间返回用户资产，则用户可以在结束后使用协商阶段中心节点的数字签名进行公示，证明服务商违背承诺。

Mixcoin 虽然保证了中心节点不会窃取混币资金，但是不能保证中心节点在混币过程中是否泄露交易信息。Velenta 等人在 Mixcoin 的基础上，引入盲签名技术，对中心节点隐藏输入地址和输出地址的对应关系，设计了 Blindcoin。图 3-4 为 Blindcoin 混币原理。与 Mixcoin 混币机制不同的是，Blindcoin 加入了盲化阶段和去盲化阶段，通过盲签名的形式，中心节点不能将交易的输入地址和输出地址进行对应，从而降低了中心节点泄漏混币交易信息的可能。

除了加入承诺机制以外，还可以通过保证金制度，降低中心节点作恶的可能。Dash 是一种匿名数字货币，同样采用混币机制保护数据隐私。在 Dash 中，中心节点想要参与混币操作，必须向系统支付 1000 个 DASH 作为押金。Dash 通过设

置押金的方式，增加了中心节点窃取混币资金的难度。

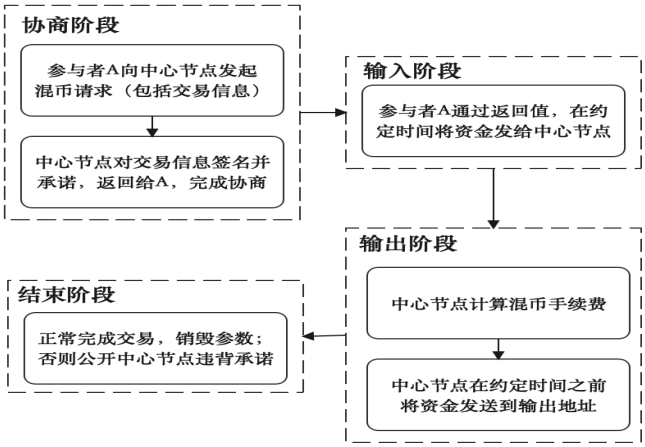

图 3-3 Mixcoin 混币原理

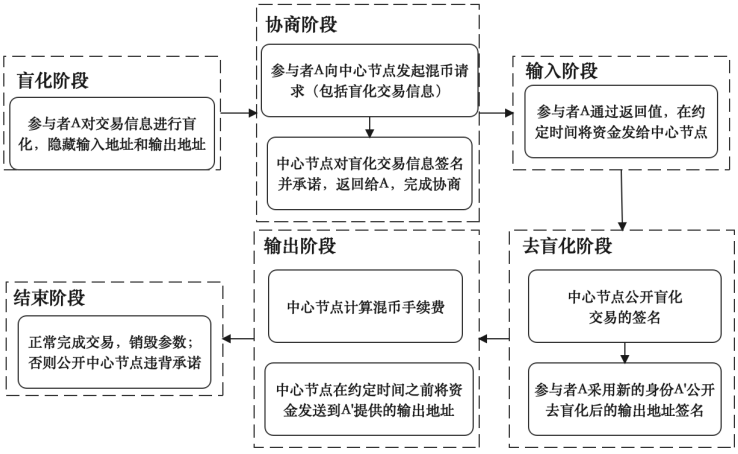

图 3-4 Blindcoin 混币原理

（2） 无中心化的混币机制

这种机制不需要中心节点进行混币操作，而是通过混币协议进行混币操作。出现最早的无中心化混币机制是 CoinJoin，由 Gregory Maxwell 首次提出。传统比特币交易中输入地址和输出地址的对应关系为一对一或者多对一，CoinJion 为了隐藏这种对应关系，将多个交易进行合并，经过合并后攻击者很难确定输入和输出的关系，因此很难分析地址间的联系以及资金的流向。CoinJoin 机制能够通过去中心化的方式增加数据隐私，可用于数字货币匿名交易中，很多研究者也在 CoinJoin 机制上提出改进。

Ruffing 等人在 CoinJoin 基础上，引入了可计数匿名组通信协议 Dissent，提出了一种新的无中心化混币机制 Coinshuffle。在 Coinshuffle 机制中，用户使用其他参与者的公钥加密自己的输出地址后发给其他参与者，其他参与者按照顺序对输出地址进行随机扰动获得新的输出地址发给下一个参与者，然后由最后一个参

与者通过自己的私钥进行解密，获得新的一组输出地址进行广播，广播后所有参与者通过新的输出地址进行资金合并创建混合交易，确定混币后指定的输出地址，完成混币交易。Coinshuffle 虽然增加数据隐私保护，但是在混币交易时，要求所有参与者同时上线，按照一定顺序完成输入地址的洗牌，这样时间开销大并且容易遭受 DOS 攻击。

3.4.2 基于加密技术的数据安全

除了混币机制还可以通过加密机制，对数据进行加密，从而实现对数据的保护。在传统区块链系统中，所有交易都是公开透明的，所有节点可以通过历史数据验证新的交易的正确性和完整性。现在通过加密技术保护隐私数据，就需要加密后的数据仍然能进行交易验证。因此，在现有的基于加密技术的隐私保护方案中，引入了安全多方计算、零知识证明以及同态加密等技术，显现加密数据的同时能够验证交易的完整性。

CoinParty 引入安全多方计算的思想，对 CoinJoin 机制进行改进。CoinParty 进行混币操作的参与者通过安全多方计算协议模拟可信第三方，在交易混合时采用椭圆曲线数字签名的方法，可以抵抗恶意对手，从而实现参与者们所有资金的安全匿名混合。Miers 等人提出了 Zerocoin，通过 RSA 累加器和零知识证明技术实现匿名交易。Zerocoin 是通过 bitcoin 与 zerocoin 之间的转换从而实现交易信息的匿名，交易者首先将拥有的 bitcoin 转换为 zerocoin，然后使用 zerocoin 支付给收款方，当交易者通过 zerocoin 的形式发起的交易出现在网络中时，验证节点通过该交易的零知识证明验证交易的合法性，如果验证通过的话代表转账成功，交易者就可以将 zerocoin 重新转换为 bitcoin。通过零知识证明的方式可以确保隐私数据的匿名性和安全性。周健等人提出引入同态加密算法，在无可信第三方的情况下，实现交易数据的多重签名。[55]

以上介绍了多种增强数据安全的机制，对这些保护机制进行总结，从是否存在可信第三方、运用机制、是否需要费用、安全性等多个角度进行对比分析，如表 3-4 所示。用表中可以看出，如果钱包方案中引入混币机制或者加密技术，能够增加数字钱包的安全性。

表 3-4 数据安全保护机制总结

机制	实例	有无第三方	混币费用	技术特点	安全性
基于混币	Mixcoin	有	需要	承诺机制	低
	Blindcoin	有	需要	盲签名+承诺机制	中
	Dash	有	需要	保证金机制	中
	CoinJoin	无	需要	多重签名	中
	Coinshuffle	无	不需要	多重签名+Dissent	中
基于加密技术	Coinparty	无	不需要	安全多方计算+ECDSA	中
	Zerocoin	无	不需要	零知识证明	高

3.5 本章小结

在本章中，首先按照私钥存储和私钥使用两种方式，对 6 类数字钱包的安全性进行比较；其次，从区块链系统出发，分析影响数字钱包安全性的两个方面，系统安全和数据安全。在系统安全问题中，因区块链系统存在一些安全漏洞，介绍了以比特币为代表的区块链系统和以太坊为代表的区块链系统中可能出现的 7 种攻击形式以及防御方法，对比分析 7 种攻击的危害程度。在数据安全中，针对传统区块链系统中交易信息公开透明的特点，对交易信息存在安全威胁，针对这一问题，提出了基于混币机制和加密技术的保护机制，通过这些机制，列出这些机制的应用实例，包括 Mixcoin、Blindcoin 等 8 种，对比分析他们的安全性。

4 一种新的门限椭圆曲线数字签名方案

4.1 引言

近几年来，通过数字钱包窃取用户数字货币的事件屡有发生，例如 2015 年 1 月黑客利用钓鱼手段盗取 Bitstamp 热钱包里的一万九千个比特币。因此，数字钱包安全对于数字货币安全以及区块链系统安全十分重要。目前，学术界对基于区块链技术的数字货币钱包的研究主要还是从用户私钥着手，设计一种如何安全生成、存储以及使用私钥的钱包。传统的数字钱包方案主要包括软件钱包、硬件钱包和托管钱包等方案，但这些钱包方案存在一个普遍的安全问题，将私钥存储在单个位置，存在单点故障威胁，容易遭受攻击。针对单点故障问题，提出一种门限椭圆曲线数字签名方案，避免单点攻击威胁。

4.2 门限椭圆曲线数字签名方案设计

本文提出的门限 ECDSA 方案主要包括三个阶段，分别是门限密钥生成、数字签名生成和数字签名验证。在门限秘密共享阶段中，通过 Shamir 联合秘密共享方案生成同态加密算法的门线密钥，在数字签名生成使用门限密钥签名，最后在验证阶段验证签名是否有效。方案整体思路如图 4-1 所示。

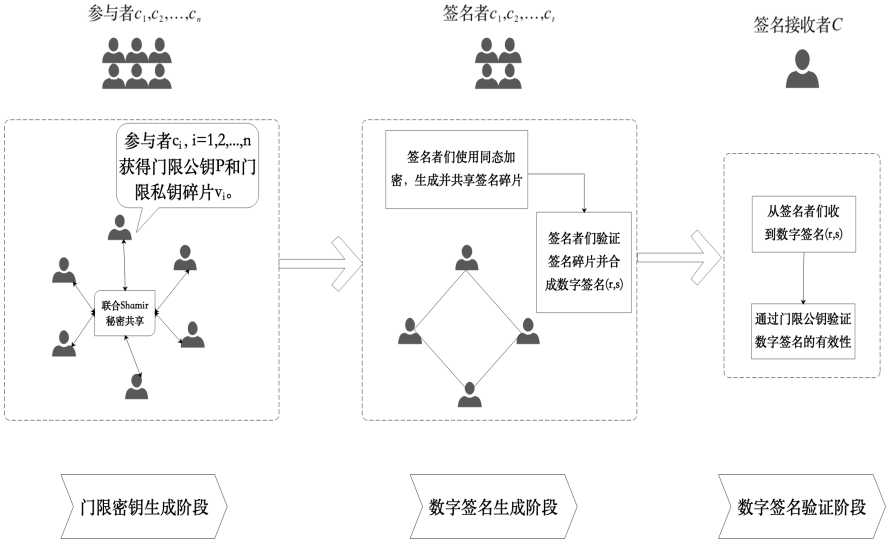

图 4-1 门限 ECDSA 方案整体思路

4.2.1 初始化

随机选取两个大素数p, q，在有限域F_p上随机选择一条椭圆曲线$E_p(a, b)$，其中G是$E_p(a, b)$的生成元，q是G的阶。假设一共有n个参与者，分别为

$C_1, C_2, \cdots, C_n$，每个参与者的标识符为$c_i, i = 1,2, \cdots, n$，其中t为门限值，不少于t个参与者可以重构秘密并参与签名。M是需要签名的消息，$H(\cdot)$是哈希函数，同态加密算法E。

4.2.2 门限密钥的生成阶段

（1） 密钥碎片生成阶段

在密钥生成阶段，所有参与者使用联合随机 Shamir 秘密共享，将自己的秘密值分成若干份的秘密份额，然后将每一个秘密份额使用安全通道发送给其他参与者，其他参与者收到秘密份额后验证其正确性，最后将收到的秘密份额整合在一起构成自己的秘密碎片，用于重构密钥。下面给出具体步骤：

参与者C_i随机选取秘密值v_0^i和多项式$f_i(x) = \sum_{l=0}^{t-1} a_{il} x^l \pmod q, i = 1,2, \cdots, n$，任意$a_{il} \in Z_q^*, l = 0,1, \cdots, t-1$，其中$v_0^i = f_i(0) = a_{i0}$，则门限私钥为$v = \sum_{i=1}^{n} v_0^i$。

参与者C_i根据式(1)计算秘密份额$f_i(c_j)$，将秘密份额$f_i(c_j)$发送给参与者C_j，并公开$A_{il} = a_{il} G, k = 0,1, \cdots, t-1$。

$$f_i(c_j) = \sum_{l=0}^{t-1} a_{il} {c_j}^l \pmod q \tag{1}$$

参与者C_j收到C_i发送的秘密份额$f_i(c_j)$后利用式(2)验证秘密份额的正确性。

$$f_i(c_j) G = \sum_{l=0}^{t-1} A_{il} {c_j}^l \tag{2}$$

若式（2）成立，则参与者C_j接受秘密份额$f_i(c_j)$；反之，拒绝秘密份额$f_i(c_j)$，并终止协议。

参与者C_j收到所有其他参与者C_i发送的正确秘密份额$f_i(c_j)$后，将所有秘密份额整合成自己的秘密碎片v_j，$v_j = \sum_{i=1}^{n} f_i(c_j) \bmod q$。

（2） 密钥重构阶段

因为门限值为t，在没有可信第三方的情况下，任意t个参与者合作就可以重构共享密钥。任意选取t个参与者构成的集合Q，不失一般性，假设$Q = \{C_1, C_2, \cdots, C_t\}$，则对应的标识符为$D = \{c_1, c_2, \cdots, c_t\}$。

计算门限私钥v。根据拉格朗日插值公式，有：

$$v = \sum_{i=1}^{n} v_0^i \pmod q = \sum_{i=1}^{n} f_i(0) \pmod q$$

$$= \sum_{i=1}^{n} \sum_{j \in D} f_i(c_j) \prod_{l=1, l \neq j}^{n} \frac{-c_l}{c_j - c_l} (\mathrm{mod} q)$$

$$= \sum_{j\in D}\sum_{i=1}^{n} f_i(c_j) \prod_{l=1,l\neq j}^{n} \frac{-c_l}{c_j - c_l} (\mathrm{mod} q)$$

$$= \sum_{j\in D} v_j \prod_{l=1,l\neq j}^{n} \frac{-c_l}{c_j - c_l} (\mathrm{mod}\ q)$$

$$= \sum_{j\in D} \gamma_j v_j \ (\mathrm{mod}\ q)$$

计算门限公钥。所有参与者C_i通过公开信息A_{il}，有：

$$P = vG = \sum_{i=1}^{n} v_0^i \, G(\mathrm{mod} q)$$

$$= \sum_{i=1}^{n} a_0^i \, G(\mathrm{mod} q) = \sum_{l=0}^{n} A_{i0} \ (\mathrm{mod}\ q)$$

（3） 密钥调用阶段

参与者C_i调用 Paillier 同态加密算法，生成自己的密钥对(X_i, Y_i)，其中私钥X_i由C_i保存，公钥Y_i公开，并生成同态加密算法E_{Y_i}。所有参与者按照密钥碎片生成步骤，生成同态加密算法E_P，解密密钥为门限私钥v。其中参与者C_i拥有加密算法E_P的门限私钥碎片v_i，$i = 1,2,\cdots,n$。

4.2.3 生成数字签名

假设参与签名的参与者就是重构共享密钥的参与者们，也就是集合Q，$Q = \{C_1, C_2, \cdots, C_t\}$。生成签名主要包括两个阶段，首先每个签名者生成自己的签名碎片，然后将所有的签名碎片合成，形成数字签名。

（1） 生成签名碎片

（1） 签名者C_i计算$m' = H(M)$，将m'转换成整数m，$i = 1,2,\cdots,t$。

（2） 签名者C_i选取随机数k_i, e_i，则整个秘密$k = \sum_{i=1}^{t} k_i$，$e = \sum_{i=1}^{t} e_i$。

（3） 签名者C_i计算$k_iG = (x_i, y_i)$，$r_i = x_i(\mathrm{mod}\ q)$，公开$k_iG$和$r_i$。则所有签名者通过公开信息，获得$kG = \sum_{i=1}^{t} k_i \, G(\mathrm{mod}\ q)$，$r = \sum_{i=1}^{t} r_i (\mathrm{mod}\ q)$。

（4） 签名者C_i计算e_ikG并公开，则$ekG = \sum_{i=1}^{t} e_i k \, G$。

（5） 所有签名者通过合作获得(ke)。

1） 签名者C_i使用同态加密算法E_{Y_i}计算$E_{Y_i}(k_i)$并发送给签名者C_j，签名者C_j计算$(E_{Y_i}(k_i)*e_j)\oplus E_{Y_i}(\omega_j^i)$，将计算结果反馈给签名者$C_i$。

2） 签名者C_j使用同态加密计算E_{Y_j}计算$E_{Y_j}(k_j)$并发送给签名者C_i，签名者C_i计算$(E_{Y_j}(k_j)*e_i)\oplus E_{Y_j}(\omega_i^j)$，将计算结果反馈给签名者$C_j$。

3） 根据同态加密算法的性质，对加密结果进行解密，签名者C_i可以获得信息$k_ie_j+\omega_j^i-\omega_i^j$，签名者$C_j$获得信息$k_je_i+\omega_i^j-\omega_j^i$。

4） 签名者C_i计算$(ke)_i=k_ie_i+\sum_{j\neq i}^{t}(k_ie_j+\omega_j^i-\omega_i^j)$并公开$(ke)_i$，则所有签名者经过计算可得$(ke)=\sum_{i=1}^{t}(ke)_i$。

（6）签名者C_i使用验证后的(ke)计算$keG(\mathrm{mod}\ q)$，判断结果与步骤(4)里的ekG是否一致，若一致说明所有签名者是诚实的，能够获得正确的(ke)；反之，说明存在不诚实签名者，则终止协议。

（2） 签名碎片合成

在生成并验证所有的签名碎片后，开始生成数字签名。在这个过程中需要确保每个签名者的签名是正确的，才能保证数字签名的有效性。下面给出签名合成的具体过程：

(1) 签名者C_i计算$s_i'=mr\gamma_iv_i(\mathrm{mod}\ q)$，并公开$s_i'G$，$i=1,2,\cdots,t$。

(2) 所有签名者通过式(3)验证s_i'的正确性：

$$\sum_{i=1}^{t}s_i'G=mrP(\mathrm{mod}\ q) \tag{3}$$

若式(3)成立，说明s_i'是正确的；反之，s_i'不正确，终止协议。

(3) 签名者C_i计算$s_i=(ke)_i+s_i'(\mathrm{mod}\ q)$，并公开$s_i$，则$s=\sum_{i=1}^{t}s_i\ (\mathrm{mod}\ q)$。

(4) 所有签名者通过式(4)验证s_i的正确性：

$$s=(ke)+\sum_{i=1}^{t}s_i'(\mathrm{mod}\ q) \tag{4}$$

若式(4)成立，说明s_i是正确的；反之，s_i不正确，终止协议。

(5) 所有签名者获得数字签名(r,s)，将数字签名(r,s)发送给签名接收者。

4.2.4 验证数字签名

签名接收者J收到数字签名(r,s)后，通过下面式子验证签名的有效性。

$$keG=sG-mPr \tag{5}$$

若等式(5)成立，签名有效；反之，签名无效。

下面给出(2,3)门限椭圆曲线数字签名方案的具体流程图，包括门限密钥生成阶段，如图 4-2 所示，数字签名生成阶段，如图 4-3 所示，共享签名验证阶段，如图 4-4 所示。

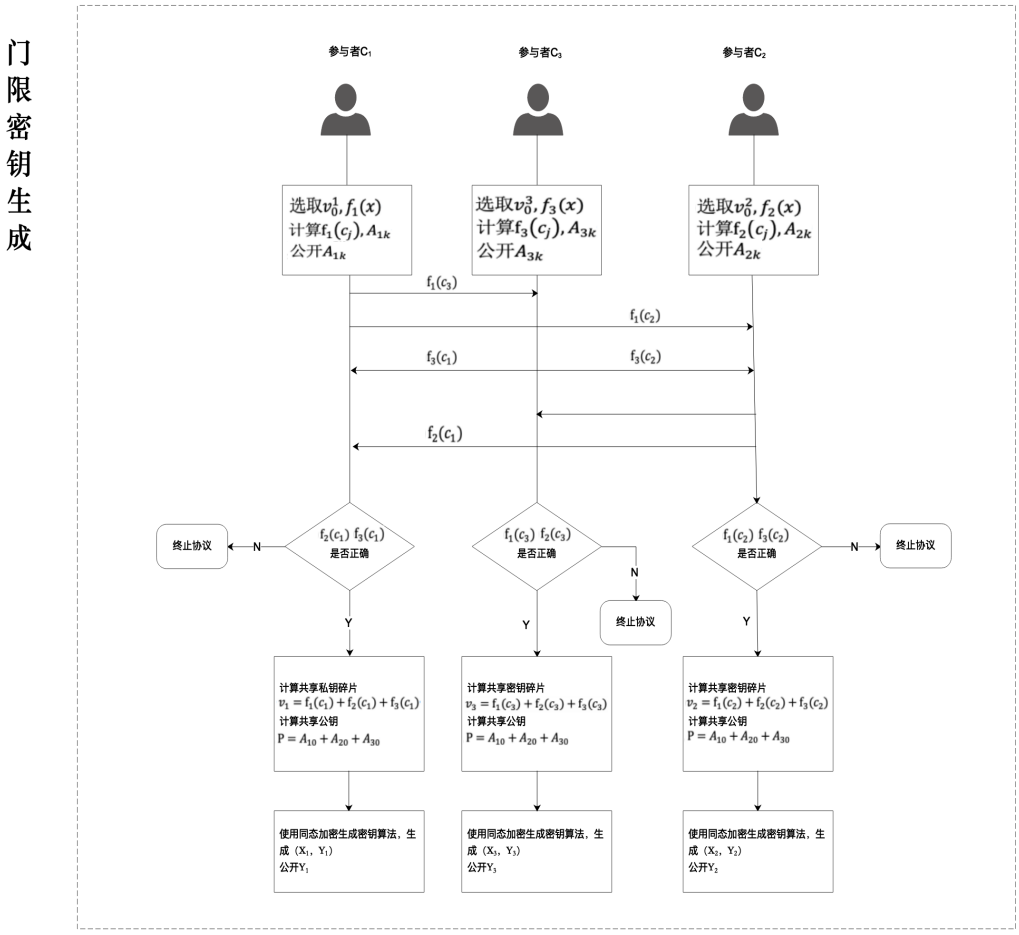

图 4-2 门限密钥生成阶段

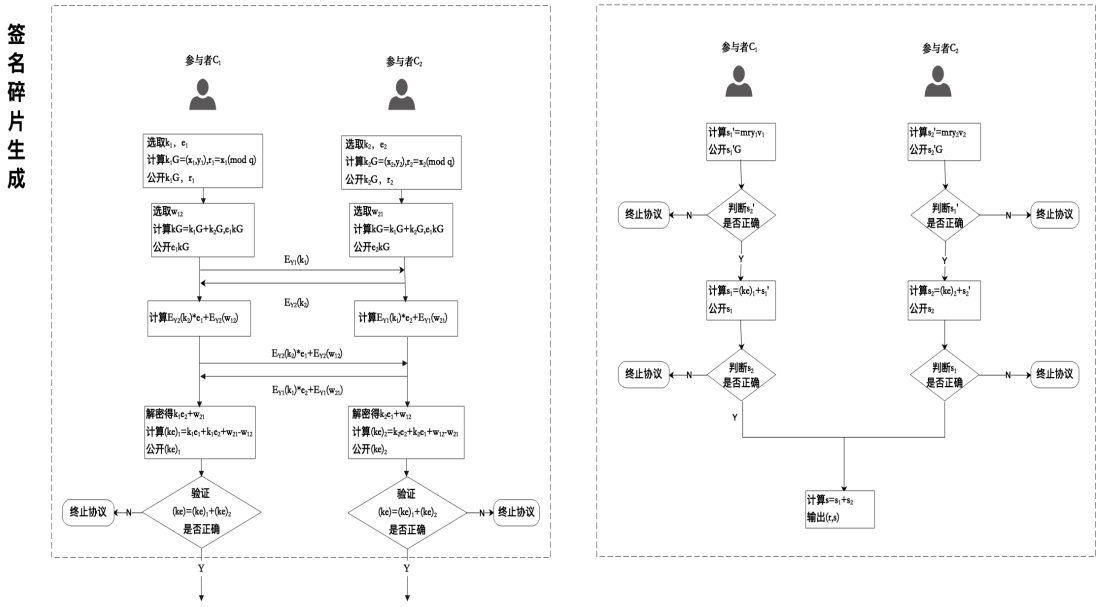

图 4-3 数字签名生成阶段

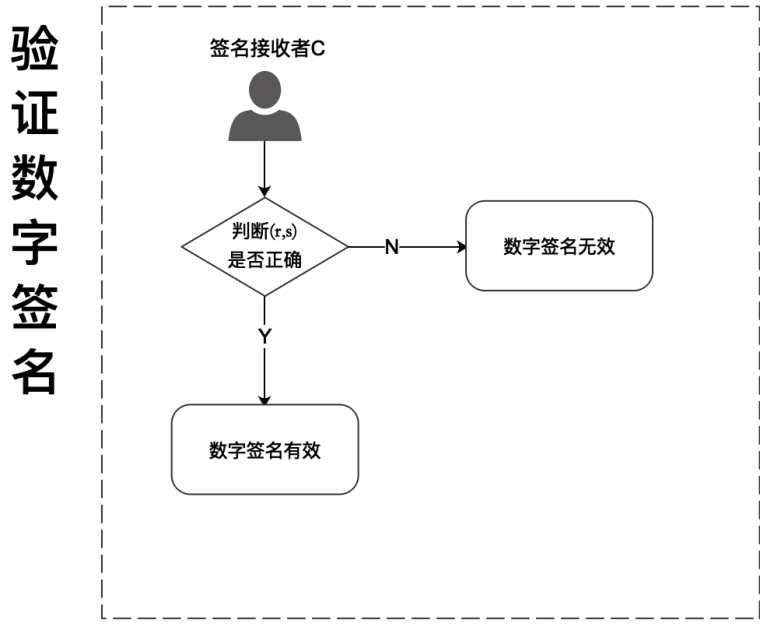

图 4-4 数字签名验证阶段

4.3 正确性与安全性分析

4.3.1 正确性

定理 1: 在密钥碎片生成阶段，任何秘密份额的正确性都可以进行验证。

证明：参与者C_i将秘密份额$f_i(c_j)$发送给C_j，公开$A_{il} = a_{il}G, i = 1,2,\cdots,n$，$C_j$收到$f_i(c_j)$后计算$f_i(c_j)G$，如果$f_i(c_j)$是正确的，必有：

$$f_i(c_j)G = f_i(x)|_{x=c_j}G(\mathrm{mod}\ q)$$

$$= \sum_{l=0}^{t-1} a_{il}c_j^l G(\mathrm{mod}\ q) = \sum_{l=0}^{t-1} a_{il}Gc_j^l(\mathrm{mod}\ q)$$

$$= \sum_{l=0}^{t-1} A_{il}{c_j}^l\,(\mathrm{mod}\ q)$$

综上，在A_{il}、c_j等信息公开的情况下，可以判断秘密份额$f_i(c_j)$的正确性。

定理 2: 在签名碎片生成阶段，签名者通过同态加密算法，可以获得完整的(ke)。

证明：签名者C_i通过同态加密算法，可以获得信息$k_i e_j + \omega_j^i - \omega_i^j$，$i = 1,2,\cdots,t$。

令

$$(ke)_i = k_i e_i + \sum_{j\neq i}^{t}\left(k_i e_j + \omega_j^i - \omega_i^j\right)$$

那么$\sum_{i=1}^{t}(ke)_i$

$$= \sum_{i=1}^{t}\left(k_i e_i + \sum_{j\neq i}^{t}\left(k_i e_j + \omega_j^i - \omega_i^j\right)\right)$$

$$= \sum_{i=1}^{t}\sum_{j=1}^{t} k_i e_j + \sum_{i=1}^{t}\sum_{j=1}^{t}(\omega_j^i - \omega_i^j)$$

$$= \sum_{i=1}^{t}\sum_{j=1}^{t} k_i e_j = \sum_{i=1}^{t} k_i \sum_{j=1}^{t} e_j = (ke)$$

每个签名者C_i计算$(ke)_i$并公开，即可得到完整的(ke)。

定理 3:在签名合成阶段，可以判断签名者是否使用正确的私钥碎片生成签名碎片。

证明：签名者C_i使用私钥碎片v_i生成s_i'，则有

$$s_i' = mr\gamma_i v_i (\mathrm{mod}\ q)$$

$$\sum_{i=1}^{t} s_i' G = s_1' G + s_2' G + \cdots + s_t' G (\mathrm{mod}\ q)$$

$$= mr\gamma_1 v_1 G + mr\gamma_2 v_2 G + \cdots + mr\gamma_t v_t G (\mathrm{mod}\ q)$$

$$= mr(\gamma_1 v_1 + \gamma_2 v_2 + \cdots + \gamma_t v_t) G (\mathrm{mod}\ q)$$

由秘密重构阶段，$v = \sum_{j\in D} \gamma_j v_j\ (\mathrm{mod}\ q)$，则有

$$\sum_{i=1}^{t} s_i' G = mrvG = mrP \tag{6}$$

综上，如果签名者C_i使用正确的秘密碎片进行签名，则必有等式(6)的成立，从而也能确定s_i'的正确性。

定理 4: 在验证签名阶段，可以验证签名的正确性。

证明：在已知消息 M 和公钥P的情况下，收到数字签名(r, s)，如果s正确，即

$$s = (ke) + \sum_{i=1}^{t} s_i' (\mathrm{mod}\ q)$$

则有

$$sG = keG + \sum_{i=1}^{t} s_i' G = keG + mrP (\mathrm{mod}\ q)$$

$$keG = sG - mrP (\mathrm{mod}\ q)$$

综上，如果计算$sG - mrP$的结果与公开的信息keG相等，说明s正确，即数字签名(r, s)有效。

4.3.2 计算安全性

设计的 ECDSA 方案是基于有限域上的椭圆曲线上离散对数问题，对于$y = xG(\mathrm{mod}\ q)$，在已知y, G, q的情况下，是不能求出x。因为有限域上的椭圆曲线上离散对数问题，除了量子攻击以外，目前还没有其他有效的解决方案。在门限密钥共享阶段，每个参与者都知道门限公钥和参数信息，以及门限私钥的碎片，都不能独自获得门限私钥，只有当超过门限值的参与者联合才能生成门限私钥。所以，该方案在计算上是安全。

4.3.3 鲁棒性

在设计的方案中，一共有n个参与者，其中t个参与签名。当参与者的数量$n \geq 2t-1$时，即使存在$t-1$个不诚实的参与者，该方案也能重构秘密并生成签名。在密钥碎片生成阶段，有验证秘密份额正确的过程，如果不诚实的参与者将错误的秘密份额发给其他诚实的参与者，诚实的参与者会进行验证，一旦验证失败就终止协议，将不诚实的参与者剔除出去。在最多剔除$t-1$个不诚实的参与者后，还剩下t个诚实参与者，通过剩下的参与者依旧能生成门限密钥。当生成门限密钥后就可以使用门限密钥生成数字签名。因此，本文方案具有鲁棒性。

4.3.4 匿名性

在设计的方案中，使用 Shamir 联合秘密共享方案，所有参加者在无可信中心的情况下，相互分享秘密份额，最后获得门限私钥碎片，私钥碎片里没有任何有关参与者的个人隐私数据，因此不会泄露个人信息。在签名碎片生成阶段，签名者两两合作，在不告知对方自己秘密值的情况下，最终每一方都获得完整秘密值(ke)。在这个过程中所有签名者通过间接的方式将信息传递给其他人，保护了自己的隐私信息。所以，在方案执行的整个过程中，没有要求输入参与者个人信息，很好的保护了参与者的隐私。因此，本文方案具有匿名性。

4.4 效率分析

上一小节对所设计的门限椭圆曲线数字签名方案进行安全性分析，本节则是对设计方案进行效率分析，主要从计算开销和算法复杂度两个方面评估方案的性能。

4.4.1 计算开销

设计方案包括生成密钥、生成数字签名以及验证数字签名三个阶段。在签名生成阶段，本方案采用杨君辉等人提出的椭圆曲线数字签名算法，将模逆运算转换成模加运算。因此，本方案中的计算主要考虑多项式计算、椭圆曲线乘法运算、调用同态加密算法时的加密运算和解密运算四种运算，如表 4-1 所示。

密钥生成阶段。每个参与者需要使用加密算法 E，构造自身在签名阶段进行加解密所需的密钥对，因此需要若干次多项式计算。并且，参与者们需要随机生成一个多项式用于生成私钥碎片和公钥，在这个过程中需要进行 3 次多项式计算和 1 次椭圆曲线乘法运算。

数字签名生成阶段。在生成参数 k,e 时，每个签名者需要进行 2 次多项式计算和 2 两次椭圆曲线乘法运算。在生成参数 ke 时，由于所有签名者关系都是对等的，假设有 t 个签名者，则每个签名者都进行 t+2 次加密运算和 t-1 次解密运算，所以总共需要t^2+2t次加密运算和t^2-t次解密运算。在生成参数 r 时，需要进行 1 次椭圆曲线乘法运算。在合成签名碎片时，需要进行 1 次椭圆曲线乘法运算。

在数字签名签证阶段，需要进行 1 次椭圆曲线乘法运算。

表 4-1 方案计算开销

	密钥生成阶段/次	数字签名生成阶段/次	签名验证阶段/次
多项式运算	若干	2	0
椭圆曲线乘法运算	1	4	1
加密运算	0	t^2+2t	0
解密运算	0	t^2-t	0

在门限密钥生成阶段，我们使用 Python 模拟了 Shamir 秘密共享方案，将秘密值分割成 n 份，设置恢复秘密值的阈值 t。然后比较了在不同秘密值分块数量 n 和阈值 t 下，秘密值分发时间的变化情况，如图 4-5 所示。

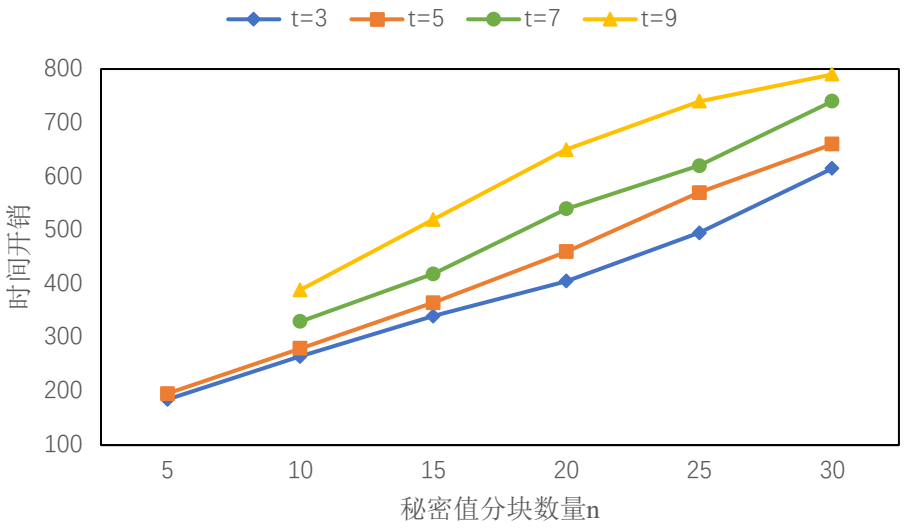

图 4-5 不同阈值下 Shamir 秘密共享方案分发秘密值时间

4.4.2 算法复杂度

本文提出的椭圆曲线数字签名方案是在李海峰等人提出的门限群签名方案的基础上进行改进的，因此在分析算法复杂度时，计算本文提出的方案、李海峰等人提出方案以及经典 ECDSA 方案的算法复杂度。[45]在计算算法复杂度时，主要从点乘、模乘和模逆运算三个指标计算生成密钥阶段、生成签名阶段和验证签名阶段的复杂度。在算法运算量计算中，假设运算的数据规模为 n，则 1 次点乘运算复杂度为$O(n^2)$，1 次模乘运算复杂度为$O(n^2 \ln n)$，1 次模逆运算复杂度约为$O(10n^2)$。表 4-2 为三种方案的算法复杂度。

表 4-2 三种方案算法复杂度

	密钥生成阶段			签名生成阶段			签名验证阶段		
	点乘	模乘	模逆	点乘	模乘	模逆	点乘	模乘	模逆
ECDSA 方案	0	0	0	1	2	1	2	2	1
文献[45]方案	3	3	0	5	2	0	4	1	0
本文方案	2	3	0	3	2	0	2	0	0

从表 4.2 可知，在密钥生成、签名生成和签名验证三个阶段中，经典 ECDSA 方案的总运算量为$O[(4\ln n + 21)n^2]$，文献[45]方案的总运算量为$O[(6\ln n + 12)n^2]$，本方案的总运算量为$O[(5\ln n + 7)n^2]$，三种方案复杂度比较如图 4-6 所示。本文方案与经典 ECDSA 方案相比，当数据规模$n < 1.2 \times 10^6$时，本文方案的算法复杂度低于经典 ECDSA 的复杂度，本文方案略优；当数据规模数量$n > 1.2 \times 10^6$时，本文方案的算法复杂度高于经典 ECDSA 方案，但本文方案的安全性更高。本文方案与文献[45]提出的方案相比，算法复杂度更低，计算效率更快。

表 4-3 给出在不同规模下，本文方案与文献[45]中方案运算复杂度之比和计算效率比。（运算复杂度比=本文方案算法复杂度/文献[45]方案算法复杂度，计算效率比=（文献[45]方案算法复杂度-本文方案算法复杂度）/文献[45]方案算法复杂度）

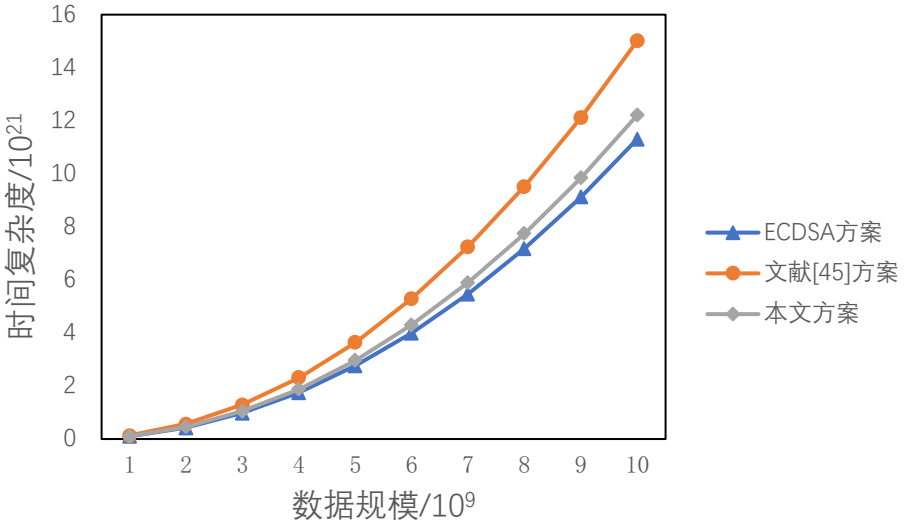

图 4-6 三种方案复杂度比较

表 4-3 文献[45]的方案与本文方案复杂度比较

n	10^3	10^4	10^5	10^6	10^7	10^8
运算复杂度比	0.7772	0.7887	0.7963	0.8017	0.8057	0.8088
效率增长率	22.28%	21.13%	20.37%	19.83%	19.43%	19.12%

4.5 本章小结

在现有的数字货币钱包中，大部分都是将私钥存储在本地数据库或者采用托管的形式存储在第三方服务器端，这两种方式都存在一个问题就是存在单点故障，攻击者很容易发起单点攻击而获得用户的私钥。本章节提出一种门限椭圆曲线数字签名方案，能够有效的防止单点故障问题。首先详细描述了生成密钥、生成数字签名和验证数字签名的过程；然后对该方案的安全性进行了分析，主要从正确性等四个方面进行安全性分析。最后通过实验的方法，从计算开销、算法复杂度两个方面评估设计方案的复杂度。

5 结论与展望

5.1 研究结论

本文对区块链、数字货币以及数字钱包当前发展现状进行阐述，针对数字钱包安全性这一问题展开研究。现有对数字钱包的研究中，缺少钱包安全性方面的文献，因此本文提出对数字钱包安全性综述性分析。然后针对传统钱包方案容易造成单点故障的问题，提出一种解决方案，通过理论分析和实验分析，验证该方案的安全性和有效性。研究结论如下：

（1）通过对数字钱包安全性分析，总结出了影响安全性的因素。通过这些因素，可以实现数字钱包方案间的安全性比较，为以后研究者们分析数字钱包安全性提供参考思路。

（2） 针对传统钱包方案存在单点故障问题，提出的门限椭圆数字签名方案引入门限共享签名技术，能够很好的解决这个问题；并且方案中加入反馈机制，能够解决传统门限签名技术中存在的合谋攻击问题。通过性能评估，发现方案中的 ECDSA 算法更加简单，但是安全性程度更高。方案与李海峰等人提出的门限群签名方案相比，算法复杂度大大降低，安全性和签名效率有所提高。

5.2 研究不足与展望

本文的研究仍然存在一些不足。首先，本文在研究数字钱包安全性时，是选取系统安全、数据安全两个方面进行定性分析，但是影响数字钱包安全性的因素还包括很多。其次，本文是提出了一种数字钱包密钥管理方案，对提出方案进行性能评估，证明适用于数字钱包的密钥管理，但是还未将方案落实在数字钱包中。

接下来的工作将围绕数字钱包的安全性继续研究，丰富影响数字钱包安全性的因素，使得数字钱包安全性的综述性分析更加全面，更加具有参考价值。同时，开始数字钱包的系统设计，加入提出的门限椭圆曲线数字签名算法，分析该方案是否能提高数字钱包的性能。

参考文献

[1] 中华人民共和国工业和信息化部.中国区块链技术和应用发展白皮书。(2016) https://www.miit.gov.cn/

[2] https://www.12371.cn/2021/03/13/ARTI1615598751923816.shtml

[3] KOGURE J，KAMAKURA K，SHIMA T，et al. Blockchain technology for next generation ICT[J]. Fujitsu Scientific & Technical Journal ，2017， 53（5）：56-61.

[4] MASON J. Intelligent contracts and the construction industry[J]. Journal of Legal Affairs and Dispute Resolution in Engineering and Construction. 2017，9（3）：04517012 .

[5] DANILIN P I，LUKIN A A，RESHETOVA E N. Assessment organization service based on ethereum platform[C]. Proceedings of the 5th Interna - tional Conference on Actual Problems of System and Software Engineering，Moscow，Russia：IEEE，2017：291-294.

[6] AZARIA A，EKBLAW A，VIEIRA T，et al. MedRec：Using blockchain for medical data access and permission management[C]. Open and Big Datainternational Conference. IEEE，2016：25-30.

[7] 余俊,张潇.区块链技术与知识产权确权登记制度的现代化[J].知识产权，2020(08):59-67.

[8] 刘佳琦,游新冬,吕学强,姜阳,李果林.区块链技术在食品溯源行业的研究[J].食品工业,2021,42(11):273-277.

[9] Nakamoto S.Bitcoin：a peer-to- peer electronic cash system[EB/OL].[2009].

[10] 巴曙松,张岱晁,朱元倩.全球数字货币的发展现状和趋势[J].金融发展研究,2020(11):3-9.

[11] http://fund.eastmoney.com/a/202201052236150090.html

[12] LiuYi, LiRuilin, LiuXingtong, et al. An efficient method to enhance bitcoin wallet security [C]//IEEE International Conference on Anti-counterfeiting, Security, and Identification (ASID), 2017:26-29.

[13] Dai Weiqi，Deng Jun，Wang Qinyuan，et al.SBLWT：a secure blockchain lightweight wallet based on trustzone[J]. IEEE Access，2018（99）：1.

[14] Wang H, Li X, J Gao, et al. MOBT: A kleptographically-secure hierarchical-deterministic wallet for multiple offline Bitcoin transactions[J]. Future generation

computer systems, 2019, 101(Dec.):315-326.

[15] Bamert T，Decker C，Wattenhofer R，et al.Bluewallet：the secure bitcoin wallet [C] // International Workshop on Security and Trust Management，2014：65-80.

[16] Bagherzandi A， Jarecki S， Saxena N， et al.Password protected secret sharing[C]//ACM Conference on Computer and Communications Security，2011：433-444.

[17] Rosario G，Steven G，Arvind N.Threshold-optimal DSA/ ECDSA signaturesand an application to bitcoin wallet security[C]//International Conference on Applied Cryptography and Net-work Security，2016：156-174.

[18] ZHOU Xiuwen, Wu Qianhong, QIN Bo, et al. Distributed bitcoin account management[C]//2016 IEEE Trustcom/BigDataSE/ ISPA. Washington D. C, USA: IEEE Press,2016:105-112.

[19] MacKenzie P，Shrimpton T，Jakobsson M.Threshold password-authenticated key exchange [J]. Journal of Cryptology，2006，19（1）：27-66.

[20] Aitzhan N Z, Svetinovic D. Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams[J]. IEEE Transactions on Dependable & Secure Computing, 2018, 15(5):840-852.

[21] ETFANS. Ethereum (12): Creating secure multi signature waller sand advanced serrings [EB/OL]. [2018-05-18].

[22] Maxwell G , Poelstra A , Seurin Y , et al. Simple Schnorr multi-signatures with app-lications to Bitcoin[J]. Designs Codes and Cryptography, 2019, 87(4).

[23] A.Shamir. How to share a secret. Communications of thr ACM, 22(1979), 612-613.

[24] Yvo Desmedt, Society and group oriented cryptography:A new concept. In Crypto’87, pages 120-127, Berlin, 1987.Springer-Verlag. LNCS No.293.

[25] 尚铭,马原,林璟锵,荆继武.SM2 椭圆曲线门限密码算法[J].密码学报,2014,1(02):155-166.

[26] 武勇,李斌.区块链安全技术体系研究[J].信息安全与通信保密,2018(07):44-52.

[27] 魏松杰,吕伟龙,李莎莎.区块链公链应用的典型安全问题综述[J].软件学报,2022,33(01):324-355.DOI:10.13328/j.cnki.jos.006280.

[28] 王凯.区块链安全综述[J].长江信息通信,2021,34(11):83-85+88.

[29] 苟俊卿,朱宇坤,王崇宇,屈宏刚,陈瑞东.面向 Libra 区块链基础设施的安全分

析与测试技术研究[J].无线电通信技术,2021,47(03):296-302.
[30]毕晓冰. 基于 iOS 的区块链数字钱包设计与实现[D].北京邮电大学,2020.DOI:10.26969/d.cnki.gbydu.2020.000812.
[31] 梁秀波,吴俊涵,赵昱,尹可挺.区块链数据安全管理和隐私保护技术研究综述[J].浙江大学学报(工学版),2022,56(01):1-15.
[32] Miers I, Garman C, et al. Zerocoin: Anonymous distributed E-Cash from bitcoin[C]//procof the 2013 IEEE SymponSecurity and Privacy(SP) Conf. Podcataway, NJ:IEEE,2013:397-411.
[33] DUFFIELD E, DIAZ D. Dash: A privacy-centric crypto-currency[EB/OL]. Https://wwww.whitepapertracker.com/wp/Dash/Dash_whitepaper.pdf. 2018.
[34] Monero. About monero[EB/OL]. [2017-06-10]. Https://getmonero.org/knowledge-base/about.
[35] Desmedt Y, Frankel Y, Shared generation of authenticators and signatures[J]. Proc Crypto, 1991.
[36] Chen T S，Hsiao T C，Chen T L． An efficient threshold group signature scheme ［C］/ /Proc of IEEE Ｒegion 10 Conference TENCON． Piscataway，NJ: IEEE Press，2004: 13-16．
[37] 彭娅． 门限数字签名理论及应用研究［D］． 广州: 中山大学，2010．(Peng Ya． Ｒesearch on threshold digital signature theory and application［D］. Guangzhou: Sun Yat-sen University，2010．)
[38] Liu Hongwei，Xie Weixin，Yu Jianping，et al． Efficiency identity- based threshold group signature scheme［J］． Journal on Communications，2009，30(5) : 122-127．
[39] 闫杰，尹旭日，张武军． 基于椭圆曲线的带门限值的群签名研究 ［J］． 东南大学学报: 自然科学版，2008，38(1) : 43-46． (Yan Jie， Yin Xuri，Zhang Wujun． Ｒesearch on group signature with threshold value based on elliptic curve ［J］． Journal of Southeast University: Nature Science Edition，2008，38(1) : 43-46.)
[40] Goldfeder S，Gennaro Ｒ，Kalodner H． Securing Bitcoin wallets via a new DSA/ECDSA threshold signature scheme［EB/OL］．(2015)［2018-07-23］． https: / /www． cs． princeton． edu / ～ stevenag /threshold_sigs． pdf
[41] Asmuth C，Bloom J． A modular approach to key safeguarding［J］． IEEE Trans

on Information Theory，1983，29(2) : 208-210．

[42] ］程宇，刘焕平． 可验证的 Asmuth-Bloom 门限秘密共享方案［J］． 哈 尔滨师范大学自然科学学报，2011，27(3) : 35-38．(Cheng Yu，Liu Huanping． The Asmuth-Bloom verifiable threshold sharing scheme ［J］． Natural Sciences Journal of Harbin Normal University， 2011，27(3) : 35-38．)

[43] Gennaro Ｒ，Jarecki S，Krawczyk H，et al． Ｒobust threshold DSS signatures ［J］． Information and Computation，2001，164(1) : 354-371．

[44] Gennaro Ｒ，Jarecki S，Krawczyk H，et al． Secure distributed key generation for discrete-log based cryptosystems［C］/ /Proc of International Conference on Theory and Application of Cryptographic Techniques． Berlin: Springer，1999: 295-310．

[45] 李海峰,蓝才会,左为平,马海云.基于身份的无可信中心的门限群签名方案[J].计算机工程与应用,2012,48(32):89-93.

[46] LI H F, LAN C H, et al. Identity-based threshold group signature scheme without trusted center[J]. Computer Engineering and Applications,2012,48(32):89-93.

[47] 周健,孙丽艳,付明.抗货币失效的区块链钱包保护协议研究[J].计算机科学与索,2020,14(12):2039-2049.

[48] 张中霞,王明文.一种适用于区块链钱包保护的无中心可验证门限签名方案[J].计算机应用研究,2020,37(S1):290-292.

[49] Mittal S, Ramkumar K R. Research perspectives on fully homomorphic encryption models for cloud sector[J]. *Journal of Computer Security*, 2021, 29(1):1-26.

[50] Alaya B, Laouamer L, Msilini N. Homomorphic encryption systems statement: Trends and challenges[J]. *Computer Science Review*, 2020, 36(8):100235.