from zero to monero

Kurt M.Alonso



摘要

加密货币区块链通常被认为是包含第三方可验证交易的分布式公共账本，无论是矿工社区还是一般用户。通常来说，交易一般需要以明文存储以便交易被公共验证。

正如我们所将要展示的，使用密码学手段能够隐藏交易双方以及交易的金额，尽管如此，这些交易依旧能够被矿工所验证以来得到共识。

目录

Intro 1

目标 1

标题 2 1

标题 2 1

# intro

区块链的目的是为了在无第三方介入的情况下，使得不相关方达成信任。

我们使用加密组建来达成信任，使得在容易访问的数据库中所保存的数据变得不可改变且不可伪造。换句话说，区块链是一个公共的分布式数据库，其中所存数据的的合法性是完整可信的。

加密货币将交易存在区块链中，区块链充当所有经过验证交易的公共账本。大多数加密货币使用明文来存储交易以便用户验证交易。

显然，一个开放的区块链违背了我们对于隐私的意愿，因为从某种程度上来说，这公开的所有用户的整个交易历史。

为了解决缺乏隐私这个问题，比特币等加密货币的用户可以使用临时的中间地址来混淆交易[1]。然而通过适当的工具可以来分析交易流，并且在很大程度上将发送方和接收方关联起来[33,14,28]。

相反，门罗币解决这一问题的方法是：通过在区块链中只存储用于接受资金的秘密的一次性地址，并且使用环签名来对每笔交易进行身份验证。有了这些方法就不存在将发送方和接收方有效链接起来的方法。[4]

除此之外，门罗中的交易金额也是被密码学方法所隐藏的，这使得货币流不再透明。

## Objective

门罗说是进来发明的货币，但他变得越来越受欢迎。不幸的是，几乎没有全面的文档来描述他所使用的机制。更糟糕的是，其理论框架的主要部分已经发布在不完整且包含错误的非同行评审的论文中。对于门罗理论框架的重要部分，只有源代码可以作为可靠的信息来源。

我们试图深入门罗的内部工作原理，查看其源代码和分析其使用的密码学方法，最后讨论他能够在多大程度上为用户提供隐私保证。

我们所做的工作基于门罗的0.11.1.0版本。这里描述的所有与交易相关的机制都属于该版本。虽然0.12.0.0是最新的版本，但是我们没有在这个报告的第一版中没有审查其多签名部分。

## 读者

我们希望读者对离散数学和代数结构有一个基本的了解，只需要密码学领域的基本见解。我们也希望读者对像比特币这样的加密货币的工作原理有基本的了解。对于以技术为导向的外行人，我们试图在脚注中填补潜在的知识空白。

我们有意省略了一些数学技术细节，或者把它们放在了脚注，当它们会妨碍清晰度的时候。我们还省略了一些我们认为不重要的具体实现细节。我们的目标是在数学密码学和计算机编程之间提出这个主题，目的是完整和概念清晰。

## 门罗币的来源

门罗币，最初被称为BitMonero，创建于2014年4月，是概念验证货币CryptoNote的衍生品。

CryptoNote是由不同的人设计的一种加密货币。2013年10月，笔名为尼古拉斯·范·萨伯哈根(Nicolas van Saberhagen)的人发表一份具有里程碑意义的白皮书以[34]。这通过一次性地址和无法被追踪的环签名为发送者和接收者提供匿名性。

自创建以来，Monero通过实现交易数量隐藏(Greg Maxwell等人在[23]中描述过)，以及Shen Noether对环签名的改进，进一步加强了它的隐私。

## 大纲

如前所述，我们的目标是提供一个自洽的和一步一步的描述Monero加密货币。本报告旨在实现这一目标，引导读者了解货币内部运作的所有要素。在我们追求全面性的过程中，我们选择了展示理解Monero复杂性所需的所有密码学元素。在第二章中，我们会谈论基本的椭圆曲线密码学。

第三章概述了与环签名相关的算法，这些算法将用于实现机密交易，同时防止double-spending攻击。

在第4章中，我们将介绍用于隐藏交易数目的密码机制。

最后，所有组件就绪后，我们将在第5章中讨论Monero中使用的交易模式。

附录A和B解释了区块链的示例交易结构，这提供了前面几节描述的理论与实际实现之间的联系。

# 基本概念

## 关于符号

是本报告的主要目标是收集、审查、纠正和统一关于门罗币内部运作的所有现有资料。同时，提供所有必要的细节，以建设性的和单线程的方式呈现材料。

实现这一目标的重要手段是满足一些标准惯例。

其中，我们使用了：

• 小写字母表示简单值、整数、字符串、位表示等

• 使用大写字母表示曲线中的点和复杂结构

对于具有特殊含义的词，我们在整个文档中尽量使用相同的符号。例如，一个曲线生成元总是用G表示，它的次数是l，私有/公共密钥尽可能分别用k/ K表示，等等。

除此之外，我们的目标是概念性展示算法和方案。具有计算机科学背景的读者可能会觉得我们忽略了一些问题，比如条目的位表示，或者在某些情况下，如何进行具体操作。

然而，我们并不认为这是一种损失。一个简单的对象，如整数或字符串，总是可以用比特字符表示。所谓的端序很少相关，主要是我们算法的约定问题。

椭圆曲线点用(x,y)表示，通常可以用两个整数表示。然而，在密码学中，通常使用“点压缩”技术，它允许只使用一个维度来表示一个点。对于我们的概念方法，不管是否使用“点压缩”，它通常都是附属的，但是大多数时候它是隐式假定的。

我们还自由地使用了散列函数，而没有指定任何具体的算法。在Monero的例子中，它通常是Keccak的变体，但是如果没有明确提到，那么它对理论来说就不重要了。

这些哈希函数将应用于整数、字符串、曲线点或这些对象的组合。这些事件被解释为位表示的散列，或者这种表示的连接。根据上下文的不同，散列的结果将是数值、位字符串，甚至是曲线点。如有需要，将提供这方面的进一步详情。

## 椭圆曲线密码学

有限域Fq，q是大于散的质数，是由集合{0，1，2，3……，q-1}构成的域。算术运算(+,\*)和一元操作都是用(mod q)^3计算。

通常,椭圆曲线被定义为点集(x,y)满足Weierstraß方程。

对于一个给定的(a, b)：

Y^2=x^3+ax+b a,b,x,y属于有限域Fq

然而，门罗币使用了一种特殊的曲线，与其他常用的NIST曲线相比，它提供了更好的安全性，以及是具有出色性能的密码原语。所使用的曲线属于扭曲爱德华兹曲线的范畴，通常表示为：

Ax^2+y^2=1+d\*x^2\*y^2 a,d,x,y属于有限域Fq

接下来，我们更喜欢第二种形式。它提供了比前面提到Weierstraß基本形式的加密原语更少的算术运算，从而这是一种更快的加密算法。详见[12]中。

设P1 = (x1, y1)和P2 = (x2, y2)是属于一个扭曲爱德华兹椭圆曲线(从今以后简称EC)的两个点。我们可以继续定义加法操作P1 + P2 = P3：

这些加法公式也适用于点加倍，即当P1 = P2时。当减去一个点是，可通过反转它的坐标(x, y)→(x，-y)并做加法得到。每当报告中出现Fq的“负”元素- x时，它实际上是-x (mod q)。

结果表明，椭圆曲线在加法运算下具有阿贝尔群结构。每次执行操作P3都是原始椭圆曲线上的一个点，换句话说，都是x3, y3 Fq。

EC中的每个点P都可以使用其自身的倍数从EC中的其他点生成一个大小为u的子群。例如，某个点ps子群可能有阶5，并且包含点(0P、P、2P、3P、4P)，每个点都在EC中。在5P处出现了所谓的在无穷处，它类似于EC上的零点，坐标为(0,1)。

方便起见，0P = 5P, 5P + P = P，这意味着子群是循环群。EC中的所有P生成一个循环子群。如果P生成一个序为素数的子群，那么所有包含的点(除了无穷点)也生成这个子群。

每一个EC的阶N等于曲线上所有点的总数，包括无穷点，由点生成的所有子群的阶都是N的因子(根据拉格朗日定理)

“引文”

想要从文件中插入图片，或者添加形状、文本框或表格？没问题！在功能区的“插入”选项卡上，点击所需选项即可。

在“插入”选项卡上查找更易用的工具，例如用于添加超链接或插入批注的工具。

## 标题 2

* 使用样式轻松快速地设置 Word 文档的格式。例如，此文本使用“列表项目符号”样式。
* 在功能区的“开始”选项卡上，查看“样式”，点击即可应用所需格式。

|  |  |  |
| --- | --- | --- |
|  | 列标题 | 列标题 |
| 行标题 | 文本 | 123.45 |
| 行标题 | 文本 | 123.45 |
|  |  |  |