现代密码学期中论文之

密码学技术在区块链中的应用

刘鹏

（云南大学 数学与统计学院信息与计算科学专业，昆明市 呈贡区 650500）

**Modern Cryptology Midterm paper:  
The Application of Cryptography Technology in Blockchain**

PENG Liu

(School of Mathematics and Statistics, Yunnan University, Chenggong District, Kunming 650500, China)

**ABSTRACT:** 区块链从本质上来说是分布式数据库，与传统数据库相比，具有数据难以篡改、信息安全性高等优势。然而如果仅仅作为数据存储的技术，其功能有限。因此人们提出将智能合约与之相结合，实现更为复杂的功能。智能合约是一套以数字形式定义的承诺，承诺控制着数字资产并包含了合约参与者约定的权利和义务，由计算机系统自动执行。将智能合约以数字化的形式写入区块链中，由区块链技术的特性保障存储、读取、执行整个过程透明、不可篡改。同时，由区块链自带的共识算法构建出一套状态机系统，使智能合约能够高效地运行。区块链中的交易打包、交易验证、区块验证等，均使用了现代密码学中的非对称加密与哈希摘要函数等技术。在加密中，比特币区块链主要使用了近年来非常流行的椭圆曲线非对称加密。

关键词：椭圆曲线加密；区块链；互联网

# 0 引言

区块链技术最初是为比特币设计的一种特殊数据库技术，它基于密码学中的椭圆曲线数字签名算法来实现去中心化的P2P系统设计。但区块链的作用不仅仅局限于比特币。现在人们在使用区块链这个词时，有时是指数据结构，有时是指数据库，有时则是指数据库技术。从数据的角度来看，区块链是一种分布式数据库(或称为分布式共享总账，Distributed shared ledger)， 这里的“分布式”不仅体现为数据的分布式存储，也体现为数据的分布式记录(即由系统参与者集体维护)；从记录效果的角度来看，区块链可以生成一套记录时间先后、不可篡改、可信任的数据库，这套数据库是去中心化存储且数据安全能够得到有效保证。具体地说，区块链技术就是一种大家共同参与记录信息和存储信息的技术。过去，人们将数据记录和存储的工作交给中心化的机构来完成，而区块链技术则让系统中的每一个人都可以参与数据的记录和存储。区块链技术在没有中央控制点的分布式对等网络下，使用分布式集体运作的方法，构建了一个P2P的自组织网络。通过复杂的校验机制，区块链数据库能够保持完整性、连续性和一致性，即使部分参与人作假也无法改变区块链的完整性，更无法篡改区块链中的数据。区块链技术涉及的关键点包括：去中心化(Decentralized)、去信任(Trustless)、集体维护(Collective maintain)、可靠数据库(Reliable data base)、时间戳(Time stamp)、非对称加密(Asymmetric cryptography)等。

区块链技术原理的来源可归纳为数学上的拜占庭将军问题。将拜占庭将军问题延伸到互联网生活中来，其内涵可概括为：在互联网大背景下，当需要与不熟悉的对手进行价值交换活动时，人们如何才能防止不会被其中的恶意破坏者欺骗和迷惑，从而做出错误的决策．而如果进一步将拜占庭将军问题延伸到技术领域中来，其内涵可概括为： 在缺少可信任的中央节点和可信任通道的情况下，分布在网络中的各个节点应如何达成共识。从这些角度来看，区块链技术解决了闻名已久的拜占庭将军问题，它提供了一种无需信任单个节点，还能创建共识网络的方法。

作为区块链技术最成功的应用， 比特币系统应用工作量证明(Proof of work, PoW)的共识机制实现交易的不可篡改性和不可伪造性。PoW共识机制的核心思想是通过引入分布式节点的算力竞争来保证数据的一致性和共识的安全性。比特币系统中，各节点基于各自的算力相互竞争，共同解决一个求解复杂但验证容易的SHA256数学难题，最快解决该难题的节点将获得区块记账权和系统自动生成的比特币奖励。具体过程如下：如果想产生一个区块并写入到区块链中，需要找到一个小于系统规定难度值的随机数，这样才可能被其他节点认可，并写入到区块链中．而找到随机数需要输出密码散列函数家族SHA256的哈希算法。其中，一个符合要求的输出值由个前导零构成。零的个数取决于网络的难度值，挖矿难度越高，零的个数会越多。当输出值不满足要求时，这个随机数就会增加一个单位，直到找到为止。找到合适随机数后，节点获得记账权和相应比特币奖励，并将该过程中产生的所有交易记录在区块上，所有区块按时间顺序连接则构成区块链。一般地，比特币系统通过灵活调整随机数搜索的难度值来控制区块的平均生成时间。

在比特币系统中，产生区块的过程称为挖矿，进行挖矿的参与者称为矿工。由于比特币系统大约每10分钟产生一个区块，这意味着大部分矿工在一定时间内很难产生区块．为了增加获得稳定收益的可能性，矿工会选择加入开放矿池进行合作挖矿。具体地，矿池中的矿工需要耗费资源尝试产生区块，即发送完整工作量证明给管理者。但完整工作量很难产生，矿工也可以选择发送部分工作量证明获得相应收益。无论哪个矿工产生区块，获得的收益将按贡献比例分配给每个矿工。参与者注册为矿工很简单，只需要提供一个公共的网络接口就可以加入开放矿池，因此开放矿池很容易受到攻击。有些注册矿工只发送部分工作量证明，当产生完整工作量证明时就会将其抛弃，这种攻击方式被称为区块截留攻击。在这种情形下，攻击者发送部分工作量证明，但不会对矿池产生有效收益，这也导致攻击者与其他矿工共同分享矿池收益，从而减少其矿池的收益。

# 1 椭圆曲线非对称加密

大多数使用公钥密码学进行加密和数字签名的产品和标准都是用RSA算法[1]。近年来，为了保证RSA使用安全性,密钥的位数一直在增加，这对于使用RSA体制的应用而言是一项巨大的负担，对进行大量安全交易的电子商务与银行系统而言更是如此。近你来出现的椭圆曲线密码学（ECC）对RSA提出了挑战。ECC的主要优势在于，它可以使用比RSA短得多的密钥得到相同安全性，减少处理荷载。

椭圆曲线并不是椭圆，之所以称之椭圆曲线为这一类方程的样式，与计算椭圆周长的方程类似，也使用三次方程来表示的。一般，椭圆曲线的三次方程形式为

其中，，，，和是实数，和是取值在实数集上的变量。在椭圆曲线加密中，并不需要这种普通形式，下述形式已经足够：

这是一个三次方程。椭圆曲线的定义中，还需要一个称作无穷远点或者零点的元素，记作。

当方程满足时，以椭圆曲线上的所有点作为集合，可以定义一种加法，进而作出一个阿贝尔群，即一个符合封闭性、加法结合律、加法单位元、逆元存在、加法交换律这5条性质的代数群。该加法是这样描述的：

（1） 无穷远点被称为该加法的单位元，在椭圆曲线上面任取一点，都有；

（2） ，其逆元为；

（3） 若椭圆曲线上的三个点在共线，则认为这三个点的和为，即若，，三点共线，则，进一步。也就是说，两个不在同一条竖直线上的点，和为与之共线且在椭圆曲线上的第三点相对于横轴的镜像对称点。

（4） 对于同一个点，计算其2倍，只需做出该点的切线，并由此寻找该切线另外的与椭圆曲线相交的点的横轴景象。

很显然，这是一个阿贝尔群（在一些其他条件下），即交换群。因为任取两点，相加的顺序与第三点存在的位置无关。

以上是实数域上的椭圆曲线描述，在椭圆曲线密码体制中，使用的变元和系数均为有限域中元素的椭圆曲线。椭圆曲线密码体制使用两种椭圆曲线，分别是适合软件实现的定义在上的素曲线（prime curve）和适合硬件实现的定义在上的二元曲线。

先讨论素曲线的情形。此时变量和系数均在里面取值

这样的代数系统可以记为。作为有限域，必然包含加法与乘法这两种运算。把ECC中的加法运算与RSA中的模乘运算相对应，将ECC中的乘法运算与RSA中的模幂运算对应。如果建立基于椭圆曲线的密码体制，需要类似因子分解两个素数之积或求离散对数这样的难题。考虑方程，其中且，对于给定的和计算比较容易，而对给定的和计算比较困难。这就是椭圆曲线的离散对数问题。

可以考虑，若给定了和，则可以通过类似快速幂取模算法的步骤，迅速得出，但是通过碰撞的方式去解，就不得不一次一次累加在上计算一次椭圆曲线加法是比较消耗时间的。若，，且，则由下列规则确定：

其中

椭圆曲线离散对数为什么难以计算？这是因为在中，如果可以取得很大，那么计算就很困难，而这里的是密码体制中的私钥，取得很大没有问题，因为并不进行私钥的传输。而模数仅是确定有限阿贝尔群中点的个数，在中，点的个数的范围是

大体上看，中点的个数约等于中元素的个数，即个。在私钥生成公钥的公式中，乘子不能比还要大，因为若，那么就是无穷远点；若，就会造成重复计算浪费计算力。

# 参考文献

[1] 周玉洁, 冯登国. 公开密钥密码算法及其快速实现 [M]. 北京: 国防工业出版社, 2002.

[2] STALLINGS W. 密码编码学与网络安全：原理与实践 [M]. 6th ed. 北京: 机械工业出版社, 2015.