国家“世界一流大学”建设高校
全 国 重 点 综 合 性 大 学
国家首批“211工程”重点建设大学

雲南大學

本科生学年论文

题　目　比特币区块链中的椭圆曲线加密方法与矿工间博弈平衡问题解析

学　　院：数学与统计学院

姓　　名：刘　　鹏

学　　号：20151910042

专　　业：信息与计算科学

指导教师：陆正福 教授

2017 年 6 月 1 日

比特币区块链中的椭圆曲线加密方法与矿工间博弈平衡问题解析

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。后来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。作为经济学与计算机科学的交叉产物，区块链技术在设计上引用了经济学中的博弈思想，从而保证整个区块链环境的健康稳定；同时以计算机科学中的数据加密技术作为网络通信与数据存储、验证的基石，而区块链采用的加密技术为近年来相对较新的椭圆曲线非对称加密技术。本文从博弈与椭圆曲线公钥体制出发，对以比特币为代表的区块链应用进行解析。

关键词：椭圆曲线加密；区块链；比特币

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[1]。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N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。

研究表明，在一个开放的矿池中，矿工可以通过攻击其他矿工增加自己的收益。如果所有矿工都选择攻击对方，那么他们获得的收益将少于他们互不攻击时获得的收益。这就是 PoW 共识算法中的挖矿困境，而这种困境也对应到博弈论中经典的囚徒困境(Prisoner's dilemma)，即攻击对个体而言是最优策略，但却不是系统最优的。如何理解和分析挖矿过程中的博弈困境无疑给比特币的发展和技术开发乃至投入使用提供了理论基础。例如 Eyal 基于博弈理论，定性地分析了挖矿过程中的困境，但并没有给出纯策略存在条件以及相应证明。本文在的基础上进一步分析矿工博弈困境的纯策略和混合策略均衡，并给出两种均衡存在的条件。

更为重要的是，PoW 共识机制存在着显著的缺陷，其强大算力造成的资源浪费（例如算力）历来为研究者所垢病，而且长达 10 分钟的交易确认时间使其相对不适合小额交易的商业应用。与此同时，随着区块链技术的发展和各种数字币的相继涌现，研究者提出多种不依赖算力而能够达成共识的机制，例如权益证明(Proof of stake, PoS)、共识授权股份证明机制(Delegated proof of stake, DPoS)共识，缠结(Tabgle)以及 Tendermint 机制。而最理想的共识算法是系统中的节点达成的共识是一个纳什均衡， 即单方面改变自己的策略都不会提高自身的收益。这为基于博弈论构建共识机制提供了新的思路。另一方面，PoW 共识过程中的挖矿困境对应经典的囚徒困境模型，其纳什均衡为互相攻击，此时的系统收益并不能达到最优。为提高系统的整体效益，有必要建立相关机制，使矿工趋向于合作，以获得较高的系统收益， 从而为实现高效的共识算法提供依据。零行列式(Zero determinant, ZD)策略是近几年在博弈论中兴起的一种新方法，它能够打破传统的纳什均衡理论。

1 文献综述

2 博弈论概要

3 矿工不主动作弊的博弈基础

4 椭圆曲线代数系统

5 椭圆曲线加密

参考文献

[1] 唐长兵, 杨珍, 郑忠龙, et al. PoW 共识算法中的博弈困境分析与优化 [J]. 自动化学报, 2017, 09): 1520-31.