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。

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 [
5 6
1
. 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