

硕 士 研 究 生 读 书 报 告



题目 密码学在区块链中的应用

作者姓名 冯天祥

作者学号 22051141

指导教师 李启雷

学科专业 软件工程

所在学院 软件学院

提交日期 二○二一 年 一 月

Application of cryptography in blockchain

A Dissertation Submitted to

Zhejiang University

in partial fulfillment of the requirements for

the degree of

Master of Engineering

Major Subject: Software Engineering

Advisor: Li Qilei

By

Feng Tianxiang

Zhejiang University, P.R. China

2021

摘要

区块链技术的发展逐渐被大众所知，但是区块链的安全性是如何保证的，其中密码学在区块链中充当着什么样的角色，对于大众来说比较遥远。本文将介绍区块链中所应用的密码学算法，以及密码学是如何保证区块链的安全性，如何保证区块链的一致性等问题进行阐述。

**关键词**：区块链技术，密码学，加密算法

Abstract

The development of blockchain technology is gradually known to the public, but how to ensure the security of the blockchain, and what role cryptography plays in the blockchain, is far away for the public. This article will introduce the cryptographic algorithms used in the blockchain, how cryptography ensures the security of the blockchain, and how to ensure the consistency of the blockchain.

**Keywords：**blockchain technology, Cryptography, encryption algorithms

## 1引言

随着区块链技术的不断发展，区块链渐渐的被大众所知。但作为普通民众的我们对于新事物总是有着一些不信任性，于是我将要介绍区块链技术的安全性保证密码学是在区块链中担任着什么样的角色的，又是如何保证区块链运行的安全和保护数据隐私的。区块链在2008年由中本聪发表的《比特币：一种点对点的电子现金系统》[1]一文中被正式提出，文中提出了一种基于点对点（Point to Point，P2P）的电子现金系统。该系统改变了基于信用的传统支付模式，而是基于密码学原理，能够使正在进行交易的双方，在意见达成一致的情况下直接进行支付，从而完全摆脱了传统的通过第三方中介进行支付来保证交易安全的模式，创造了一种全新的电子货币体系。

2 区块链技术简介

区块链技术是利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算范式。简单来讲，在区块链系统中，每过一段时间，各参与主体产生的交易数据会被打包成一个数据区块，数据区块按照时间顺序依次排列，形成数据区块的链条，各参与主体拥有同样的数据链条，且无法单方面篡改，任何信息的修改只有经过约定比例的主体同意方可进行，并且只能添加新的信息，无法删除或修改旧的信息，从而实现多主体间的信息共享和一致决策，确保各主体身份和主体间交易信息的不可篡改、公开透明。

如图 1[2]为区块链的基本框架：

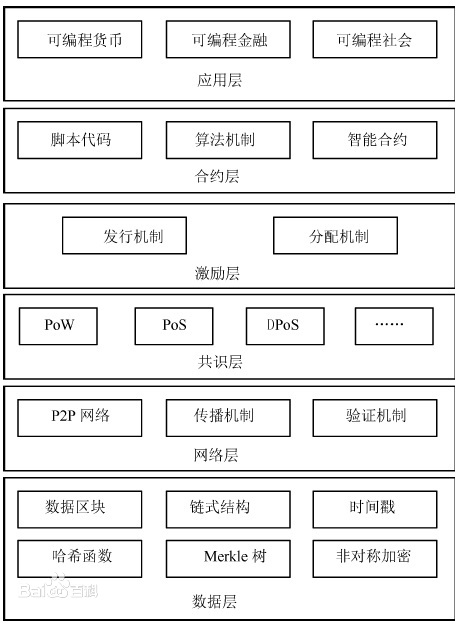


图 1 区块链基本框架图

数据层:该层封装了底层数据区块的链式结构，以及公钥密码技术、时间戳、Merkle树以及哈希函数，这是整个区块链技术中最底层的数据结构。区块链将这些技术结合在一起，构成了安全可靠的新型存储模式。

网络层:该层采用了P2P网络、传播机制和验 证机制。P2P技术使得区块链具有自动组网功能，传播机制和验证机制明确了消息传播协议和数据验证方法，具体协议和方法取决于实际应用场景。通过传播机制和验证机制，区块链中每个节点均可参与数据校验和记账。

共识层:该层是区块链系统中的核心技术，该层采用的共识协议包括:工作量证明PoW(Proof of Work)、权益证明PoS( Proof of Stake) 、股份授权证明DPoS(Delegated Proof of Stake)等。

激励层:为了鼓励更多节点参与到区块链运作，该层采用经济激励机制，设计了相应的激励发行机制和分配方法。同时，惩罚不遵守规则的节点，使得整个系统朝着良性循环的方向发展。

合约层:该层封装了各类脚本代码、算法机制和智能合约，使得区块链具有可编程属性。比特币具有脚本编写功能，以太坊具有更强的编程功能。通过算法机制和编程，用户能够实现具有各种功能的 智能合约。智能合约通常被认为是一个自动担保账户，例如，当特定的条件满足时，程序就会自动执行，完成相应的功能。

应用层:该层封装了区块链的各种实际应用需求和实现案例，例如，可编程货币、可编程金融、可编 程社会等。[3]。3 密码学在区块链中的应用

本节以比特币为例说明密码学在区块链中的实际应用点。

## 3.1 哈希函数

哈希函数[4](Hash function)是指将任意长度的字符串映射到固定长度为的字符串，记为。哈希函数可以认为是在映射集合中查找对应的值，如果不在该映射集合中，那么计算数，并且在上述映射集合中将赋值给。一个有效的哈希函数通常具有以下特点:

1) 抗修改性，改动任意一位时，变动较大;

2) 不可逆性，已知，得到的概率较低;

3) 抗碰撞性，对于任意和，的概率极低。

在区块链中，哈希函数主要用于数据完整性、数据加密、共识计算的工作量证明、区块之间链接等。区块链采用了双 SHA256、RIPEMD160 等哈希函数，SHA256 主要用于加密交易形成区块，RIPEMD160则用于生成比特币的地址。区块链系统中的双SHA256函数是将不同长度的消息经过两次SHA256计算处理，输出256位二进制字符串统一存储。哈希函数被用来确保区块链中信息的完整性，在存储、传输的过程中，使得信息不会被篡改，以及篡改后能及时发现。另外，哈希函数在区块链的另外一个应用 是作为区块间相连的哈希指针，如图 2所示。

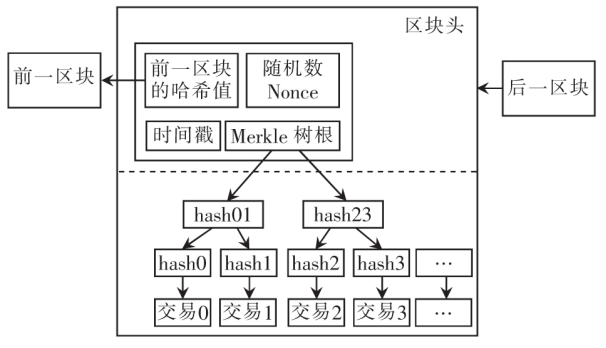


图 2 区块内部结构

区块可以看作以哈希值为地址的指针，当前区块包含这上一个区块的哈希值，，因此，每个区块不但链接前一个区块的位置，也提供一个哈希值去验证这个区块 所包含的数据的完整性。

默克尔树(Merkle Tree)[5]是一种用哈希函数建立的二叉树结构，在区块链的 数据区块中数据结构主要为二叉Merkle树，每个交易记录对应于一个哈希值，并对应于Merkle树的叶子节点，两个叶子节点再次两两配对哈希计算，通过递归的方式直到最后一个哈希值作为Merkle 树根存入区块体。如图 2 所示，叶子节点hash0、hash1分别存储交易0、交易 1的哈希值，非叶子节点hash01存储其子节点的哈希值，根节点通过计算其子节点的值得到。在区块链中，用户通过区块头得到Merkle树根和别的节点所提供的中间哈希值来验证某个交易是否存在于区块中。利用哈希函数的抗碰撞性和抗修改性，只要Merkle树根确定，那么所有的数据块都不可被篡改。

## 3.2 非对称密码算法

非对称加密算法的加解密过程由两个密钥完成：公开密钥（public key：简称公钥）和私有密钥（private key：简称私钥）。非对称加密算法的基本流程是：甲方生成一对密钥，私钥由甲方安全保管，公钥公开给所有人，乙方使用公钥将数据加密后发送密文给甲方，甲方用私钥进行解密。在整个通信过程中，不存在密钥安全传输的问题。常见的非对称加密算法有 RSA 算法[6]、ECC算法[7]、国密 sm2 算法[8]等。比特币中的公私钥对采用256位ECC算法，私钥可随机产生，公钥由私钥计算获得，但从公钥无法计算出私钥。比特币的公钥为椭圆曲线算法生成的65字节的随机数，再经过SHA265、RIPEMD160算法生成20字节长度的消息摘要作为比特币地址的主体信息，再在前面加上版本号信息，在末尾添加4个字节的地址校验码，地址校验码通过对摘要结果进行两次SHA256运算得到，取哈希值的前四位产生，最后把版本信息、主体信息和地址校验码放在一块通过Base58转换为易识别的字符串作为地址。

非对称加密算法在区块链中的重要应用就是作为数字签名[9]存在。数字签名是手写签名的数字模拟，主要包含密钥生成、签名、验证签名三个过程。公钥与私钥是通过密钥生成算法得到的一个密钥对，公钥是密钥对中公开的部分，私钥则是非公开的部分。密钥生成算法保证了仅通过公钥来计算私钥是非常困难的，这在很大程度上保证了用户私钥的安全性。在区块链中，公钥即是账户地址，一个人可以拥有多个公钥，每个公钥均为与用户真实身份无关的随机数字，他人无法通过公钥推导出用户的真实身份，从而保护了用户隐私。一个被验证通过的〈消息,签名>对能够保证:该消息是该公钥的所有者发送的——消息源身份认证;该消息没有被任何人篡改过——消息内容的完整性;该公钥的所有者无法否认他发送过该消息——消息内容不可否认性。

数字签名具体算法如下：

1. 密钥生成。通过算法生成公钥和私钥，公钥对所有人公开，私钥由签名者自己保存；
2. 签名算法。签名者利用私钥生成对消息的签名，然后把<消息,签名>对公布出去；
3. 验证算法。所有人都可以利用签名者公布的公钥对该<消息,签名>对进行验证，验证结果为通过或不通过。

椭圆曲线签名算法(ECDSA)为比特币中使用的数字签名算法。该算法在有限域上的椭圆曲线中进行运算，设私钥、公钥分别为、，其中为椭圆曲线的基点。使用私钥签名和使用公钥验证签名的过程如下:

私钥签名：

1. 选择随机数，计算点；
2. 根据随机数、消息的哈希、私钥，计算；
3. 将消息和签名发给接收方。

公钥验证签名：

1. 接收方收到消息和签名；
2. 根据消息求哈希；
3. 使用发送方公钥计算并于比较，如相等即签名验证成功。

# 4 共识算中的密码学

区块链本质是一个分布式账本，如何在分布式系统中高效地达成共识是分布式计算领域的重要研究问题.正如社会系统中“民主”和“集中”的对立关系相似，决策权越分散的系统达成共识的效率越低、但系统稳定性和满意度越高;而决策权越集中的系统更易达成共识，但同时更易出现专制和独裁。区块链技术的核心优势之一就是能够在决策权高度分散的去中心化系统中使得各节点高效地针对区块数据的有效性达成共识。

比特币中采用高度依赖节点算力的工作量证明(Proof of work,PoW)[10]机制来保证比特币网络分布式记账的一致性。

PoW共识:中本聪在其比特币奠基性论文中设计了PoW共识机制,其核心思想是通过引入分布式节点的算力竞争来保证数据一致性和共识的安全性。比特币系统中，各节点(即矿工)基于各自的计算机算力相互竞争来共同解决一个求解复杂但验证容易的SHA256数学难题(即挖矿)，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。该数学难题可表述为:根据当前难度值，通过搜索求解一个合适的随机数(Nonce)使得图 2 中区块头各元数据的双SHA256哈希值小于或等于目标哈希值。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为10分钟左右。一般说来，PoW共识的随机数搜索过程如下。

1. 搜集当前时间段的全网未确认交易,并增加一个用于发行新比特币奖励的Coinbase交易，形成当前区块体的交易集合；
2. 计算区块体交易集合的Merkle根记入区块头,并填写区块头的其他元数据，其中随机数Nonce置零；
3. 随机数Nonce加1；计算当前区块头的双 SHA256哈希值,如果小于或等于目标哈希值，则成功搜索到合适的随机数并获得该区块的记账权；否则继续(3)直到任一节点搜索到合适的随机数为止；
4. 如果一定时间内未成功，则更新时间戳和未确认交易集合、重新计算Merkle根后继续搜索。

符合要求的区块头哈希值通常由多个前导零构成，目标哈希值越小，区块头哈希值的前导零越多，成功找到合适的随机数并“挖”出新区块的难度越大。据区块链实时监测网站Blockchain.info显示，截止到现在，符合要求的区块头哈希值一般有19个前导零，例如第668020号区块哈希值为“000000000000000000023767fcd5e30fe9cfdef83563b1a395b3a725f6e2ed07”。按照概率计算，每16次随机数搜索将会有找到一个含有一个前导零的区块哈希值，因而比特币目前19位前导零哈希值要求次随机数搜索才能找到一个合适的随机数并生成一个新的区块。由此可见，比特币区块链系统的安全性和不可篡改性是由PoW共识机制的强大算力所保证的，任何对于区块数据的攻击或篡改都必须重新计算该区块以及其后所有区块的SHA256难题，并且计算速度必须使得伪造链长度超过主链，这种攻击难度导致的成本将远超其收益。

# 5 密码学安全性保证

## 5.1 数据安全性

比特币涉及的数据主要包括三类：交易、区块、区块链，分别采用了不同的安全机制，具体内容如下：

(1) 交易数据安全性。解锁脚本包含账户所有 者的数字签名（基于公钥算法 ECC），确保交易数据无法伪造。

(2) 区块数据安全性。区块头引入Merkle根字段（基于哈希算法SHA256），用于验证区块中是否存 在某交易；区块创建采用工作量证明机制（POW），提 高了新区块创建的难度和成本。

(3) 区块链数据安全性。区块头引入父区块哈希值，确保所有区块连接形成完整的单链条（分叉现象属于临时状态），且从任意区块均可回溯至第一个区块；将创世区块作为第一个区块，确保区块链具有信任锚（信任起点）；基于每个节点独立选择累计工作量最大的区块链（去中心化共识），使得区块深度（该区块后面的区块数）越大越难被分叉篡改，可有效避免共识攻击，确保不出现双重支付或伪交易（被撤销）

## 5.2 账户安全性

私钥是使用账户资金（比特币）的唯一条件，一旦丢失（如意外删除或硬盘损坏）或被他人窃取或劫持，账户资金将无法使用或被他人花费，因此只要保护好私钥，就可确保账户资金的安全性。私钥保护主要采用以下几种方式：

1. 加密私钥。使用AES算法先使用口令将私钥加密，然后使用Base58Check进行编码。加密后私钥可以保存在钱包中或备份介质里。
2. 硬件钱包。加密私钥以计算机文件形式存在，容易被恶意软件窃取后采用暴力方式破解。为避免私钥被黑客窃取，可采用智能硬件形式保护私钥，如CPU IC卡或USB Key；私钥只允许在硬件中按需生成，并通过硬件自身的安全机制确保私钥不允许以任何形式导出硬件之外。

# 6 总结

区块链中的交易和区块实体都涉及到公钥加密、数字签名、哈希函数等多种密码学组件。为了满足更高的隐私保护需求，一些区块链方案还需要环签名、零知识证明等隐私保护技术。这些密码学组件的安全性直接影响到区块链数据层的安全性。短期来看，数学理论、密码学解析和计算技术的发展不会对一些已经形成标准的密码算法构成威胁。采用的密码算法主要包括：SHA256，RIPEMD160，ECC256，AES256，其安全性已经过长期实践验证。但是随着量子计算的兴起,现有的密码算法将面临安全性降低甚至被攻破的危险。尽管现阶段量子计算的研究成果还不能对区块链中的密码算法构成威胁，但是从长远看，区块链的发展势必要引入可以抵抗量子攻击的加密系统。

参考文献

1. Nakamoto Satoshi. Bitcoin: A peer-to-peer electronic cash system[J]. Consulted,2009.
2. https://baike.baidu.com/item/区块链/13465666
3. 袁勇,王跃飞.区块链技术发展现状与展望[J].自动化学报,2016,42(4):481-494.
4. Katz, J. and Lindell, Y. (2007) Introduction to Modern Cryptography (Chapman & Hall/CRC Cryptography and Network Security Series). Chapman & Hall/CRC, Stanford.
5. Merkle R C . A Digital Signature Based on a Conventional Encryption Function[C]// Conference on the Theory and Application of Cryptographic Techniques. Springer, Berlin, Heidelberg, 1987.
6. R. L. Rivest, A. Shamir, L. Adl eman. A method for obtaining digital signatures and public key cryptosystems[J]. Communications of the ACM, 1978, 21(2): 120-126.
7. D. Hankerson, A. Menezes. Elliptic curve cryptography [M]. Springer US, 2011, 397
8. X. Han, B. Wang, A. Wang, et al. Algorithm-Based Countermeasures against Power Analysis Attacks for Public-Key Cryptography SM2[C]. 2014 Tenth International Conference on Computational Intelligence and Security (CIS), Kunming, 2014, 435-439
9. Diffie W . New Direction in Cryptography[J]. IEEE trans. Inform. Theory, 1976, 22.
10. Dwork C , Naor M . Pricing via Processing or Combatting Junk Mail[J]. 1992.