**重庆邮电大学《计算机网络》课程报告**

**2024-2025学年第 1 学期**

**题 目 区块链技术及其应用**

**姓 名 陈俊宏**

**学 号 2022211758**

**专 业 计算机科学与技术**

**班 级 04012202**

**成 绩**

**2024年 12月 20日**

区块链技术及其应用

**摘 要：**区块链是一种广泛应用于新兴数字加密货币的去中心化基础架构，随着比特币的逐渐被接受而受到关注和研究。区块链技术具有去中心化，区块数据基本不可篡改、去信任化等特性，因此受到企业尤其是金融机构的追捧。阐述了区块链技术的核心技术原理，探讨了区块链技术的应用以及所存在的监管问题、安全问题，旨在对区块链技术的相关研究提供帮助。。

**关键词：**区块链；数字货币；去中心化；分布式；共识机制

1引言

区块链是比特币的基础支撑技术，首次出现在中本聪（Satoshi Nakamoto）发表的《比特币：一种点对点式的电子现金系统》[1]，文中详细描述了如何建立一套全新的、去中心化的、不需要信任基础的点到点交易体系的方法，其可实现性已经被自 2009 年运行至今的比特币所证明大赛。

2 区块链的基本概念

2.1 什么是区块链？

区块链这一概念最早是在中本聪的比特币白皮书［１］中 提出的，但它不是以区块链出现的，而是以工作量证明链的形式存在。下面是中本聪对区块链概念的叙 述：时间戳服务就是通过对区块中数据项加上时间戳进行哈希，并把这一哈希值广泛地传播出去，就像是新闻或者在 世界性新闻网络上的发帖一样。显然，要得到这个 哈希值，就需证明在过去的某个时刻加上时间戳的数据必然存在。每个时间戳包含了先前的时间戳，这样就形成了一条链，并且后面的时间戳都对前一个时间戳进行了增强。

3 区块链的部分基础技术

3.1哈希算法

哈希（也称为散列）算法将任意长度的输入值映射为较短的固定长度的二进制值。例如，SHA256算法就是将任意长度的输入映射为长度为256位的固定长度输出，这个二进制值称为哈希值（也称为散列值）。数据的哈希值可以检验数据的完整性，一般用于快速查找和加密算法。

哈希算法广泛应用于区块链中,区块链通常不保存原始数据，而是保存该数据的哈 希 值，Merkle树中的节点信息是两次 SHA256哈希运算得到的。以太坊账户址，是用

哈希运算一个公钥得到的;而比特币地址，则是通过SHA256和 RIPEMD160哈希运 算一个公钥而得到的。此外，签名频繁应用于区块链中，它由私钥和需要被签名的数 据经哈希运算而成。著名的工 作 量 证 明 算 法、Merkle树都是哈希算法的应用。

3.2 Merkle树

Merkle树是由Ralph Merkle发明的一种基于数据哈希构建的树：１）其数据 结构是一棵树，一般为二叉树，也可以为多叉树；２）其叶子节点是数据块（如文件或文件集合）的哈希值；３）非叶子节点是其所有子节点的哈希值。Merkle树在验证文件对比中应用较多，特别是在分布式环境下，Merkle树会大大减小数据的传输量和计算的复杂度。

3.3 P2P网络技术

P2P网络技术又称为点对点技术，它是一个没有中心服务器、依靠用户群交换信息的互联网体系。P2P网络由于没有中心化服务器，使得它天生具有耐攻击、高容错的优点；并且各个节点地位平等，服务分散在各个节点上进行，因此部分节点或网络遭到攻击对整个系统几乎没有影响。比特币系统应用P2P技术，使各个节点独立地参与系统，每个节点都是一个独立的个体，单独节点宕机或者遭到攻击都不会对系统造成影响。

4 区块链的特性

（１）可靠开放性：区块链的设计使它能够有效预防故障与攻击，５１％攻击除外（如果攻击者拥有网络中５１％的算力，他就可以对区块进行伪造，然后自己又最快地计算出正确的解，造成区块链分叉，达到攻击的目的）。所有参与系统的用户享一个公共区块链，不会存在因为单点失效而导致系统故障的情况，从而保证了系统的可靠性和数据的可获得性。

（２）信息透明性：网络上的任何节点都可以查看整个账本。由于记录的交易信息不包含任何隐私，因此任何记录在册的信息都可以被查看，保证了数据的透明性。

（３）不可更改性：区块链系统采取的是完全冗余的策略，所有完整节点都有一份完整数据，要想更改某一区块的数据，必须保证所有完整节点数据被修改，这个情况几乎不可能发生，因此降低了欺诈的风险。

（４）不可逆转性：交易不存在撤销操作，交易一旦被验证

认可，就不可再逆转。

5 区块链技术的瓶颈

区块链技术存在如下瓶颈。

（１）过大的完整账本的存储空间。现在，比特币区块链的 容量达到了８０ＧＢ，并且还在逐日增加，对于想要运行完整区 块链的节点来说这无疑是一个很大的挑战。

（２）信息分发采用全网广播。这是一种洪泛式，要求网络 性能好。

（３）交易效率低下。比特币交易效率主要受到两个方面 的影响：

１）区块产生时间；

２）区块大小。现在的比特币交易速 度为７笔／秒，不适合处理实时交易。 （４）算力浪费。整个系统中，只有成功得到区块合法记账 权的那部分算力得到了奖励的回报，其他算力都是做无用功， 浪费巨大。

（５）单个节点独自升级，升级成本高。

6 区块链的主要技术平台与应用

6.1以太坊

Ethereum（以太坊）是一个平台和一种编程语言，使开发人员能够建立和发布下一代分布式应用。其在２０１３年由Vitalik Buterin提出，它的目的是为建立去中心化的应用创建一种可替代的协议，给一大类的去中心化的应用程序提供一组不同的平衡机制，这对需要快速开发、安全性要求低、很少使用的应用程序以及在不同应用之间能有效互动很重要。以太坊是一个编程平台，它提供了各种模板，用户只需要把以太坊提供的各种模板链接到一起就能搭建自己的应用。因此，在以太坊上创建应用的成本大大减少、速度大大提高，这也造就了以太坊成为区块链中最好的项目之一。具体来说，以太坊通过一种图灵完备的脚本语言（EVM语言）来创建应用，类似于汇编语言，但编写以太坊应用并不需要直接使用ＥＶＭ，而是使用Solidity，Serpent，LLL类编程语言，再通过编译器转换成EVM语言供以太坊平台使用。开发者可以通过以太坊这一平台创建自己的区块链应用。一般来讲，以太坊上有３种应用：

１）金融应用，包括电子货币、金融衍生品、对冲交易合约、存储钱包、遗嘱，甚至是一些最终的完善就业合同；

２）半金融应用，这类应用涉及金钱，但不是完全看重金钱，也有重要的非金钱的应用，一个典型的例子就是为解决计算问题的自实施奖励；

３）非金融应用，例如在线投票和去中心化管理。。

6.2 智能合约

区块链技术的智能合约是一组情景——应对型的程序化规则和逻辑，是部署在区块链上的去中心化、可信息共享的程序代码。签署合约的各参与方就合约内容达成一致，以智能合约的形式部署在区块链上，即可不依赖任何中心机构自动化地代表各签署方执行合约。智能合约具有自治、去中心化等特点，一旦启动就会自动运行，不需要任何合约签署方的干预。

7 结论

区块链技术的发展被业内人士广泛看好，这个越来越受青睐的趋势会一直持续，这些趋势不一定以区块链的形式直接出现，可能会作为区块链技术的衍生品兴起。区 块链应用已经从最初单纯的数字货币过渡到更广泛的金融业，并且渗透到社会中的很多领域，比如身份验证、跨境支付、文件存储、物联网等，其中金融领域是目前最成熟、应用最广的领域。区块链技术作为当下最热门的技术之一，值得我们投入更多的时间与精力进行学习和研究。

参考文献

1. Roy C K, Cordy J R, Koschke R. Comparison and evaluation of code clone detection techniques and tools: A qualitative approach[J]. Science of Computer Programming, 2009, 74(7): 470-495.
2. Buterin V. Ethereum: A next generation smart contract and decentralized application platform [EB/OL]. <https://github.com/ethereum/wiki/wiki/White-Paper>, 2013.Koponen T, Casado M, Gude N, et al. Onix: A distributed control platform for large-scale production networks[Z]. 2010.
3. Szydło M. Merkle tree traversal in log space and time[J]. Lecture Notes in Computer Science, 2004, 3027: 541-554.