

硕 士 研 究 生 读 书 报 告



|  |  |
| --- | --- |
| **题目** | **比特币与区块链技术** |
| 作者姓名 | 戴毅 |
| 作者学号 | 22051415 |
| 指导教师 | 李启雷 |
| 学科专业 | 电子信息 |
| 所在学院 | 软件学院 |
| 提交日期 | 二○ 21 年 1月 |

BitCoin and Blockchain Technology

A Dissertation Submitted to

Zhejiang University

in partial fulfillment of the requirements for

the degree of

Master of Engineering

Major Subject: Software Engineering

Advisor: QiLeiLi

By

YiDai

Zhejiang University, P.R. China

2021

摘要

本文从比特币出发，对区块链技术进行了概览式的探讨和总结。2008年由中本聪第一次提出了区块链的概念[1] ，在随后的几年中，区块链成为了电子货币比特币的核心组成部分：作为所有交易的公共账簿。通过利用点对点网络和分布式时间戳服务器，区块链数据库能够进行自主管理。为比特币而发明的区块链使它成为第一个解决重复消费问题的数字货币。本文从比特币中的区块链技术提炼出区块链的精华，并说明了二者之间的联系与脉络。

**关键词**：区块链，比特币

Abstract

The paper Starts from Bitcoin, providing an overview discussion and summary of blockchain technology.

In 2008, Satoshi Nakamoto first proposed the concept of blockchain[1]. In the following years, blockchain became the core component of the electronic currency Bitcoin: as the public account book for all transactions.

Through the use of peer-to-peer networks and distributed time stamp servers, blockchain databases can be managed autonomously.

The blockchain invented for Bitcoin makes it the first digital currency to solve the problem of repeated consumption.

This paper extracts the essence of the blockchain from the blockchain technology in Bitcoin, and explains the connection and context between the two.

**Keywords：**Bitcoin，Blockchain

# 1引言

互联网上的贸易，几乎都需要借助金融机构作为可资信赖的第三方来处理电子支付信息。虽然这类系统在绝大多数情况下都运作良好，但是这类系统仍然内生性地受制于“基于信用的模式”(trust based model)的弱点。我们无法实现完全不可逆的交易，因为金融机构总是不可避免地会出面协调争端。而金融中介的存在，也会增加交易的成本，并且限制了实际可行的最小交易规模，也限制了日常的小额支付交易。并且潜在的损失还在于，很多商品和服务本身是无法退货的，如果缺乏不可逆的支付手段，互联网的贸易就大大受限。因为有潜在的退款的可能，就需要交易双方拥有信任。而商家也必须提防自己的客户，因此会向客户索取完全不必要的个人信息。而实际的商业行为中，一定比例的欺诈性客户也被认为是不可避免的，相关损失视作销售费用处理。而在使用物理现金的情况下，这些销售费用和支付问题上的不确定性却是可以避免的，因为此时没有第三方信用中介的存在。[1]

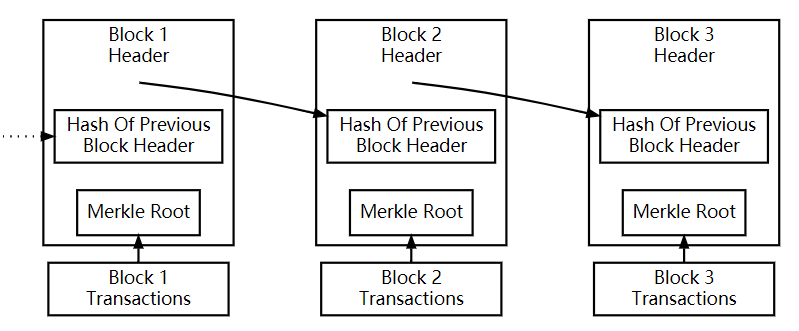
比特币作为一种电子支付系统，基于密码学原理而不基于信用，使得发生交易行为的双方能够直接进行支付。这种方式可以杜绝回滚支付交易的可能，从而保护特定的商家与买家。这种通过点对点分布式的时间戳服务器来生成依照时间前后排列并加以记录的电子交易证明，现如今有统一的名称：区块链技术。

此篇读书报告中，我通过阅读一些比特币与区块链领域的学术论文或者白皮书，对比特币和区块链的技术细节有体悟，并且对二者之间联系进行详细的阐述。

# 2 比特币中的区块链技术

区块链提供比特币的公共分类账、交易的有序和时间戳记录。此系统用于防止重复支出和修改以前的交易记录。[2]

比特币网络中的每个完整节点独立存储一个块链，仅包含由该节点验证的块。当多个节点的块链中具有相同的块时，它们被认为是一致的。这些节点为维持共识而遵循的验证规则称为共识规则。

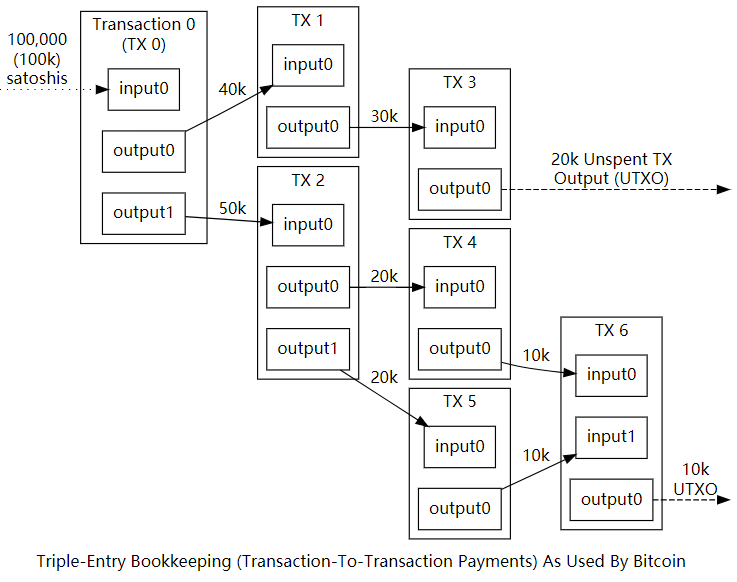


区块链简单示例

上图显示了块链的简化版本。一个或多个新事务的块将收集到块的事务数据部分。每个事务的副本都进行哈希处理，然后对哈希进行配对、哈希处理、再次配对并再次哈希，直到单个哈希保持为 merkle树的 merkle 根。

merkle 根存储在块标头中。每个块还存储上一个块标头的哈希值，将块链接在一起。这可确保在不修改记录事务的块以及以下所有块的情况下无法修改事务。

事务也链接在一起，每个事务都使用以前在一个或多个早期事务中接收的 satoshis，因此一个事务的输入是上一个事务的输出。



事务流动示例

单个事务可以创建多个输出，就像发送到多个地址时一样，但特定事务的每个输出只能在块链中用作输入一次。任何后续的引用都是禁止的双重消费，即两次尝试花同样的沙托希。[2]

输出绑定到事务标识符 （TXID），即已签名事务的哈希值。

由于特定事务的每个输出只能花费一次，因此块链中包含的所有事务的输出都可以分类为未用事务输出 （UTXOs）或已花费的事务输出。要使付款有效，它必须仅使用 UTXOs 作为输入。

忽略硬币基础交易（稍后描述），如果交易的输出值超过其输入，交易将被拒绝， 但如果输入超过输出的值， 任何价值差异可能会被创建包含该交易的块的比特币矿工声称为交易费用。 例如，在上面的图示中，每笔交易的花费比从组合投入中收到的少花费 10000 个 satoshis，实际上支付了 10000 个 satoshi 交易费用。

# 3 比特币与区块链技术的联系

区块链技术是比特币的底层技术，也是比特币的核心与基础架构。比特币一直在没有任何中心化机构运营和管理的情况下运行，区块链技术是从比特币技术抽象提取出来的，或者称之为分布式账本技术。[3]

# 4 小结

比特币是一种P2P形式的数字货币，P2P（即点对点）的传输意味着一个去中心化的支付系统; 区块链是一种去中心化的分布式账本数据库。去中心化，即与传统中心化的方式不同，这里是没有中心，或者说人人都是中心；分布式账本数据库，即每个节点都参与整个账本的变动记录，并同步共享复制整个账本的数据。

比特币被创造出来时，还没有出现“区块链”这个名词。之后，随着比特价格的大涨以及比特币系统多年的平稳运行，人们才开始关心比特币系统背后的技术，归纳总结出了“区块链技术”的概念。

当区块链技术被挖掘出来以后，人们发现这项技术实在太强大了，不仅仅可以用来开发类似于比特币之类的数字货币，稍加完善甚至可以应用到互联网涉及的各个领域。

形象点理解，区块链技术相当于水，比特币相当于水里长出的一种鱼。

**参考文献**

1. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[R]. Manubot, 2019.
2. Cornelius.Block Chain[EB/OL].https://developer.bitcoin.org/devguide/block\_chain.html,2019-5-20.
3. 云计算那点事.一文读懂：比特币和区块链是什么关系？[EB/OL].https://www.sohu.com/a/233392961\_404292,2018-05-30.