比特币技术调研报告

|  |  |  |  |
| --- | --- | --- | --- |
| 更新日期 | 版本说明 | 更新人 | 备注 |
| 2018.07.13 | v0.1，设计目录结构 | 乔嘉林 |  |
|  |  |  |  |

目 录

[一、 概述 3](#_Toc519245136)

[二、 去中心化 3](#_Toc519245137)

[2.1 非对称加密 3](#_Toc519245138)

[2.2 数字签名 3](#_Toc519245139)

[三、 数据模型 3](#_Toc519245140)

[2.3 账单（Transaction） 3](#_Toc519245141)

[2.4 区块（Block） 3](#_Toc519245142)

[四、 隐私保护 3](#_Toc519245143)

[五、 写入流程 4](#_Toc519245144)

[六、 冲突解决 4](#_Toc519245145)

[七、 区块链的局限 4](#_Toc519245146)

## 概述

本文档主要介绍了比特币的产生背景，以及比特币系统的设计思想与原理。面向的读者为有一定计算机、数据库基础知识的技术人员。

比特币是首个得到大规模部署的区块链技术应用。2008年，中本聪提出了比特币的白皮书《Bitcoin: A Peer-to-Peer Electronic Cash System》，2009年比特币系统上线运行，至今稳定运行了9年时间，从系统稳定性角度看，是一个非常成功的分布式系统了，无论在信息技术历史还是在金融学历史上都具有十分重要的意义。比特币项目在诞生和发展过程中，借鉴了来自数字货币、密码学、博弈论、分布式系统、控制论等多个领域的技术成果，本文的两位作者方向分别为分布式存储系统和密码学。

## 去中心化

### 非对称加密

### 数字签名

## 数据模型

### 账单（Transaction）

### 区块（Block）

## 隐私保护

## 写入流程

## 冲突解决

## 区块链的局限