

# 理想



## [理想\\_下载链接1](#)

著者:[加]维塔利克·布特林

出版者:科学出版社

出版时间:2019-5-1

装帧:

isbn:9787030609816

本书梳理了以太坊创始人维塔利克·布特林（Vitalik Buterin）创立区块链平台以太坊6年以来的技术思想，对以太坊技术实现、共识机制、可扩展

性、隐私保护等热门话题的探讨和思考，以及区块链技术在经济博弈、去中心化方面的见解。

全书分为5卷，共收录了51篇技术文章，内容涉及 权益证明、去中心化自治、客户端、终化、有限理性、可扩展性、超理性、 $P+\epsilon$ 攻击、分叉、Casper、ZK-SNARK、ZK-STARK、Plasma、区块链治理、容错等 关键理论和技术。

本书适合区块链技术领域智能合约、分布式计算、数字货币相关的从业人员和管理者阅读。

作者介绍:

Vitalaik: 以太坊创始人

目录: 卷 (2013-2014年)

以太坊：下一代智能合约和去中心化应用平台

创建去中心化自治公司 (I)

创建去中心化自治公司 (II)：与外界交互

创建去中心化自治公司 (III)：身份公司

刀手：一种惩罚性的权益证明算法

论交易费用与市场化解方案的谬误

谢林币：只需小信任的通用数据反馈

DAO、DAC、DA及其他：一个不完整的术语指南

向12秒区块时间发展

软件和有限理性

论可扩展性 (I)：顶层构建

论可扩展性 (II)：超立方体

探索稳定的加密货币

论比特币的高纲领主义以及货币和平台的网络效应

权益证明的可行性：如何学会热爱弱主观性？

秘密共享DAO：加密2.0

论孤岛

第二卷 (2015年)

轻客户端和权益证明

超理性和DAO

$P+\epsilon$ 攻击

主观性/可利用性权衡

愿景：区块链技术的价值

论公有链和私有链

论反预言揭示博弈

论慢速出块和快速出块

第三卷 (2016年)

论结算 终化

加密经济学和X风险研究人员应该多互相倾听

以太坊2.0紫皮书

一种权益证明的设计哲学

ZK-SNARK (I)：二次方程式算术编程

第四卷 (2017年)

参数化Casper：去中心化、终化时间、开销之间的权衡

ZK-SNARK (II)：椭圆曲线配对的探索

ZK-SNARK (III)：算法迷踪

去中心化的含义

小削减条件  
动态验证者集合下的安全性  
通过边际价格歧视来推动慈善事业  
硬分叉、软分叉、默认和强制  
通过协调问题来实现工程安全  
代币众筹模式分析  
伤害三角形  
论梅特卡夫定律、外部性和生态系统分裂  
Plasma：可扩展的自主智能合约  
以太坊协议的史前史  
论交易媒介代币的估值  
无状态客户端  
ZK-STARK（I）：多项式证明  
ZK-STARK（II）：核心证明  
第五卷（2018年）  
小可行Plasma  
权益证明问答  
Plasma现金：少量用户数据检查的Plasma  
以太坊分片问答  
ZK-STARK（III）：攻坚  
99%容错共识指南  
并行化Lamport 99%容错共识  
CBC Casper教程  
• • • • • ([收起](#))

[理想 下载链接1](#)

## 标签

区块链

新经济

ETH

## 评论

-----

[理想 下载链接1](#)

书评

-----  
[理想 下载链接1](#)