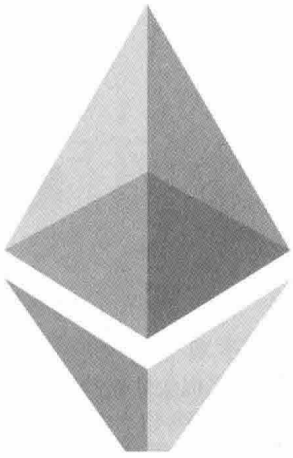
灵钛科技
独角时代
联合出品

理·想

以太坊的区块链创世录

〔加〕维塔利克·布特林 著

科学出版社



理想

以太坊的区块链创世录

〔加〕维塔利克·布特林 著

科学出版社

北京

内 容 简 介

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、最终化、有限理性、可扩展性、超理性、$P+\varepsilon$ 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。

图书在版编目（CIP）数据

理·想：以太坊的区块链创世录/（加）维塔利克·布特林（Vitalik Buterin）著. —北京：科学出版社，2019.5

ISBN 978-7-03-060981-6

Ⅰ.理… Ⅱ.维… Ⅲ.电子商务-支付方式-研究 Ⅳ.F713.361.3

中国版本图书馆CIP数据核字（2019）第066998号

责任编辑：喻永光 杨 凯 / 责任制作：魏 谨

责任印制：张克忠

北京东方科龙图文有限公司 制作

http://www.okbook.com.cn

科学出版社 出版

北京东黄城根北街16号

邮政编码：100717

http://www.sciencep.com

天津文林印务有限公司 印刷

科学出版社发行 各地新华书店经销

*

2019年5月第 一 版 开本：16 787×1092

2019年5月第一次印刷 印张：27 1/2

字数：650 000

定价：128.00元

（如有印装质量问题，我社负责调换）

推荐序

区块链、比特币、加密货币、以太坊、密码学……除非你不问世事多年，否则在这些年里，你耳边一定无数次萦绕过这些话语。在你拿到这本书的此刻，虽然我并不了解你是谁、你从何而来，但我敢打赌你一定对这一切已有所听闻。

你是一位研究计算机科学的学生？

还是一位经济学家？

一位商人？

或者是一位职业投资人？

你也许是一位热切期盼改变世界的理想主义者？

你可能是一位高校学者？

一位IT领域的专业人士？

一位淘金热的追寻者？

或许，仅仅是因为你那聪慧又好奇的灵魂一直在催促你前进。

我无法知道你获知这一切的来源。你可能从报纸和杂志第一次听说这些陌生的名词；也可能是博客和YouTube？嗯……可能还有Twitter？Reddit？微信？众多大大小小的博客和论坛？又或者是书中的黄金屋指引你到达这里？或许这些方式你都有所涉及吧。

我想做出一个大胆的猜测，这几年你也一定听说过各种各样的想法和意见：

“这玩意儿毫无用处，都是骗人的！”

“这玩意儿压根就是泡沫！”

“加密货币是通向财务自由的捷径！”

“这项技术将改变整个世界！”

“区块链将颠覆银行系统和传统企业！”

“这是无政府主义者妄图打破世界经济格局的狼子野心！”

“比特币统领一切！”

“比特币现金才是真正的比特币！”

“滚蛋，比特币现金SV才是地球的唯一希望！”

“以太坊才是未来！”

“幼稚，看我波场吊打以太坊！”

“数风流人物，还看XXXX！”

“以太经典才是原汁原味的以太坊！”

你越是充满好奇和激情地深入探究，你越不知道你该相信谁。但我希望你能够通过本书找到一个答案。

本书收录了以太坊创始人维塔利克·布特林（Vitalik Buterin）从2013年到2018年的优秀作品。维塔利克出生于俄罗斯，在加拿大的多伦多长大。2011年，他开始研究比特币，

并为比特币底层的数学原理、理念以及技术深深着迷，从此不可自拔。此后，维塔利克联合有志之士创办了《比特币杂志》，并充当该杂志的主要编辑和作者。2013年秋，他提出了“以太坊”概念。

在众多聪慧的头脑以及志同道合者的帮助下，以太坊得以面世，并掀起一股巨大的创新浪潮，同时也带动了一波模仿、投机与投资交杂的热潮。从那以后，维塔利克成了各大媒体的常客。

除了作为以太坊基金会的首席科学家，维塔利克还是一位高产的演说家和作家。他撰写了许多很重要同时也十分复杂的文章，话题涉及密码学、经济学、区块链可扩展性等。他尽最大的努力试图让这些内容变得简单易懂，让更多人能够理解其中的含义。

阅读本书不会使你一夜暴富，更不可能让你一夜之间成为密码学和区块链大师。但它能够帮助你在这个日益重要且人类认知仍在快速增长的领域拥有立足之地。

我还想借着这个机会告诉那些四处造谣的人：

维塔利克不是外星人，他是百分之百纯正的地球人。

他不是一个骗子。

他没有用三个月速成一口流利的普通话，那是长年累月的坚持和辛勤努力的结晶。

他也不是什么亿万富豪，更没有什么贴身侍从或者保镖。

你问我怎么知道这么多？因为我是他的父亲，我们共同走过25载岁月。

当我写这段话时，维塔利克在旁边和我聊起本书。我很好奇这些年是什么一直激励着他孜孜不倦地撰写这些文章。但对维塔利克来说，这些都只不过是自然而然的结果——他花了大量的时间去思考，然后分享，仅此而已。

过去，维塔利克会在全球各地分享很多早期的新想法。而现在，这些新想法大多会发表在EthResearch论坛（http://ethresear.ch），以供社区的小伙伴们共同讨论。维塔利克更倾向于在个人博客中发表经过自己细致思考及验证的思路和看法。当然，也正如你所见，许多文章在发表前会先行得到小伙伴们（如卡尔·弗洛尔斯、贾斯汀·德雷克等）热情的评论与审阅。每一次发表文章过后，维塔利克都很重视文章底下的每一句评论。他乐于与读者展开讨论，这种来自于社区的头脑风暴不亚于又一次深刻的思考。

我尝试着刺探后续的文章主题，维塔利克是这样回答我的：“可能会有很多重复的主题，如权益证明、可扩展性、Plasma、零知识证明、擦除码等。我也可能会从哲学和经济学的角度撰写更多文章。过去我在一些媒体访问时会进行一些关于人际交互、社会和组织架构的评论，但现在很少这么做了。毕竟，在这些领域，我的想法和观点很难进行逻辑论证。”

问起维塔利克对本书的期望，他说：“我希望这本书能够给更多人带来启发，同时吸引更多有志之士加入以太坊社区，甚至是更广泛的加密经济学领域。与此同时，我也希望读者不仅能通过本书了解当下的以太坊，还能更深入地了解我们所追求的更广阔的未来”。

他还提到“……我会一直在我的个人博客（vitalik.ca）、Twitter@VitalikButerin以及Reddit（user vbuterin）进行写作。欢迎大家随时向我抛出问题”。

那就这样吧！请开始你的阅读之旅：去思考，去参与，为这片奇妙的新大陆贡献你的一份力量！

Dima Buterin

目 录

第一卷（2013–2014 年）

以太坊：下一代智能合约和去中心化应用平台 …… 2
创建去中心化自治公司（Ⅰ） …… 26
创建去中心化自治公司（Ⅱ）：与外界交互 …… 30
创建去中心化自治公司（Ⅲ）：身份公司 …… 35
刀手：一种惩罚性的权益证明算法 …… 40
论交易费用与市场化解决方案的谬误 …… 43
谢林币：只需最小信任的通用数据反馈 …… 47
DAO、DAC、DA 及其他：一个不完整的术语指南 …… 52
向 12 秒区块时间发展 …… 58
软件和有限理性 …… 68
论可扩展性（Ⅰ）：顶层构建 …… 78
论可扩展性（Ⅱ）：超立方体 …… 85
探索稳定的加密货币 …… 96
论比特币的最高纲领主义以及货币和平台的网络效应 …… 105
权益证明的可行性：如何学会热爱弱主观性？ …… 115
秘密共享 DAO：加密 2.0 …… 124
论孤岛 …… 138

第二卷（2015 年）

轻客户端和权益证明 …… 146
超理性和 DAO …… 152
$P+\varepsilon$ 攻击 …… 158
主观性 / 可利用性权衡 …… 163
愿景：区块链技术的价值 …… 170

论公有链和私有链 ……178
论反预揭示博弈 ……181
论慢速出块和快速出块 ……185

第三卷（2016 年）

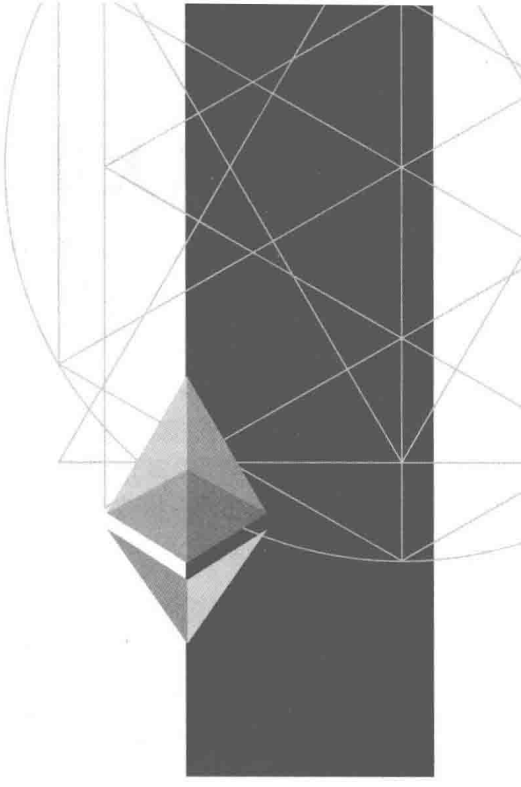
论结算最终化 ……197
加密经济学和 X 风险研究人员应该多互相倾听 ……203
以太坊 2.0 紫皮书 ……206
一种权益证明的设计哲学 ……219
ZK-SNARK（Ⅰ）：二次方程式算术编程 ……222

第四卷（2017 年）

参数化 Casper：去中心化、最终化时间、开销之间的权衡 ……232
ZK-SNARK（Ⅱ）：椭圆曲线配对的探索 ……236
ZK-SNARK（Ⅲ）：算法迷踪 ……243
去中心化的含义 ……248
最小削减条件 ……254
动态验证者集合下的安全性 ……261
通过边际价格歧视来推动慈善事业 ……269
硬分叉、软分叉、默认和强制 ……272
通过协调问题来实现工程安全 ……276
代币众筹模式分析 ……280
伤害三角形 ……288
论梅特卡夫定律、外部性和生态系统分裂 ……291
Plasma：可扩展的自主智能合约 ……295
以太坊协议的史前史 ……333
论交易媒介代币的估值 ……339
无状态客户端 ……342
ZK-STARK（Ⅰ）：多项式证明 ……345
ZK-STARK（Ⅱ）：核心证明 ……352

第五卷（2018 年）

最小可行 Plasma ……362
权益证明问答 ……365
Plasma 现金：更少单用户数据检查的 Plasma ……381
以太坊分片问答 ……383
ZK-STARK（Ⅲ）：攻坚 ……403
99% 容错共识指南……418
并行化 Lamport 99% 容错共识 ……422
CBC Casper 教程……423



第一卷
（2013–2014年）

- **2013年**

11月，维塔利克·布特林（Vitalik Buterin）撰写了以太坊白皮书的第一版初稿。事实上，初稿并非严格的白皮书，只是一份针对万事达币（Mastercoin）的提案——在万事达币的基础上增加智能合约。

两周后，维塔利克通过电子邮件在其朋友圈内传播这份初稿，并招募开发人员，以太坊的创始团队就此诞生。

- **2014年**

1月23日，维塔利克在其创办的《比特币杂志》（*Bitcoin Magazine*）上正式发布以太坊白皮书《以太坊：下一代智能合约和去中心化应用平台》。

1月25日，维塔利克在比特币迈阿密会议上正式公布以太坊。

2月，以太坊社区建设、代码、Wiki（多人协作写作系统）以及法律趋于完善。为了创建合适的基础结构并取得法律支持，团队决定将原定于2014年2月举行的以太币预售延期。此后，以太坊团队开始全身心投入项目研发，备战主网上线。

3月，以太坊发布第三版测试网络（PoC 3），并将总部搬到了瑞士楚格州。

4月，以太坊联合创始人加文·伍德（Gavin Wood）发布了被誉为“以太坊技术圣经”的黄皮书，明确以太坊虚拟机（EVM）的技术规范。根据说明，以太坊客户端至少支持C++、Go、Python、Java、JavaScript和Haskell编程语言。

6月，以太坊基金Stiftung Ethereum在瑞士楚格州设立。该基金旨在合规化管理众筹募集的资金，服务于以太坊以及去中心化技术生态。

同月，以太坊发布第4版测试网（PoC 4）。

7月，以太坊发布第5版测试网络（PoC 5），并正式开启为期42天的众筹，最终募得3.1万比特币（时值1840万美元）。

10月，以太坊发布第6版测试网络（PoC 6）。在这一版本的测试网络中，区块速度从60秒缩减到了12秒，并且使用了新的基于GHOST的协议。

11月，第一届以太坊开发者会议DEVCON 0在德国柏林举行。在这次会议中，很多项目成员第一次见面，通过Skype发言。

以太坊：下一代智能合约和去中心化应用平台

（2013 年 11 月）

编者按

2014年1月23日，维塔利克在其创办的《比特币杂志》上正式发布以太坊白皮书。以太坊白皮书从比特币系统结构切入，引出了以太坊的全新设计、应用场景，并对费用、中心化等经济学、哲学问题进行了解答。

2009年1月，中本聪（Satoshi Nakamoto）首先将比特币区块链带上现实舞台，同时引入两个未经测试的颠覆性的概念。第一个是“比特币”，一种去中心化的点对点在线货币，它能够在没有任何资产担保、内在价值或者中心发行者的前提下维持价值。到今天，比特币聚焦了越来越多的公众视线——不管是作为一种没有中央银行背书的货币所造成的政治影响，还是其剧烈的价格波动。然而，中本聪这一伟大试验还有另一个重要部分——通过工作量证明使人们可以就交易顺序达成共识的“区块链”概念。作为一项应用，比特币可以被认为是一个先申请系统（first-to-file）：如果某个实体拥有50 BTC（Bitcoin，比特币），并且同时把这50 BTC发送给A和B，此时，只有最先确认的交易才会生效。但想要从两笔交易中分辨出先后，并没有内在的方案。这个问题多年来一直阻碍着去中心化数字货币的发展。中本聪的区块链是第一个可靠的去中心化解决方案。如今，开发者们开始将注意力转向区块链，以及怎样将区块链应用于货币以外的领域。

人们常提及的应用包括使用链上数字资产代表定制性货币和金融工具（如彩色币）、基础物理设备的所有权（如智能财产）、诸如域名等的不可替代性资产（域名币），以及诸如去中心化交易所、金融衍生品、点对点赌博、链上身份与声誉系统等更为高级的应用。另一个重要领域是智能合约，即可依据任意预先制定的规则自动转移数字资产的系统。例如，某人有一个资金合约，该合约形式表述为“A每天最多可提现X个货币单位，B每天最多可提现Y个货币单位，而A和B一起可提取任意数量的货币单位，并且A可冻结B的提现权”。如果把这种合约的逻辑进一步扩展，就是去中心化自治组织（Decentralized Autonomous Organization, DAO），即一系列长期包含某个组织的资产并对组织章程进行编码的智能合约。以太坊的目标就是提供一条内置成熟的图灵完备编程语言的区块链。这种编程语言可用来创建合约，以编码任意状态转换的功能。用户只需要使用代码编写逻辑，就能构建出上述系统，以及更多有待发掘的新功能。

历　史

去中心化数字货币的概念，就像其他应用，比如财产登记，早在几十年前就被提出来了。20世纪八九十年代的匿名E-Cash协议是以大卫·乔姆（David Chaum）的盲签名技术

为基础的。此协议提供具有高度隐私性的货币，但并没有流行起来，因为它们依赖于中心化的中介。1998年，戴伟（Wei Dai）的B-Money首次引入了通过解决计算难题和去中心化共识来创造货币的想法，但该提议并未给出实现去中心化共识的具体方法。2005年，哈尔·芬尼（Hal Finney）引入了“可重复使用的工作量证明机制”的概念，该机制同时结合了B-money的想法和亚当·拜克（Adam Back）提出的计算困难的哈希现金难题以创造加密货币。但是，这种概念再次迷失于理想化，依赖于可信任的计算作为后端。

因为货币是一个先申请应用，交易的顺序至关重要，所以去中心化的货币需要找到实现去中心化共识的解决方法。在比特币之前的所有货币的协议遭遇的主要障碍是，尽管关于创建安全的拜占庭容错多方共识系统的研究已历时多年，但上述协议只解决了一半问题。这些协议假设系统内的所有参与者是已知的，从而获得诸如“如果有N个参与方加入到系统中，那么系统可以容忍$N/4$个恶意参与者”这类形式的安全边际。而这个假设的问题在于，在匿名的情况下，这些所谓的安全边际很容易就会受到“女巫”攻击。因为一个攻击者可以在一台服务器或者僵尸网络上创建成千上万的节点，并利用这些节点单方面获取多数份额。

中本聪的创新在于引入了一个理念：将一个非常简单的基于节点的去中心化共识协议与工作量证明机制结合。节点通过工作量证明机制获得参与到系统中的权利，每10分钟将交易打包到区块中，从而创建出不断增长的区块链。尽管拥有大量算力的节点有更大的影响力，但获得比整个网络更多的算力比创建100万个节点要困难得多。尽管比特币区块链的模型非常简陋，但实践证明它确实非常好用。在未来5年，它将成为全世界两百多种货币和协议的基石。

■ 作为状态转换系统的比特币

从技术角度来讲，比特币账本可以被认为是一个状态转换系统（图1），该系统包含所有现存的比特币的所有权状态和一个状态转换函数。其中，状态转换函数以当前状态和交易为输入，从而输出新的状态。例如，在标准的银行系统中，状态就是一张资产负债表。一个从A账户向B账户转账X美元的请求是一笔交易。状态转换函数将从A账户中减去X美元，并向B账户增加X美元。如果A账户的余额小于X美元，那么状态转换函数就会返回一个错误提示。因此，可以定义状态转换函数为`APPLY(S,TX)->S'`或`ERROR`。

在上述银行系统中，状态转换函数如下：

```
APPLY({Alice:$50,Bob:$50},"send $20 from Alice to Bob")={Alice:$30,Bob:$70}
```

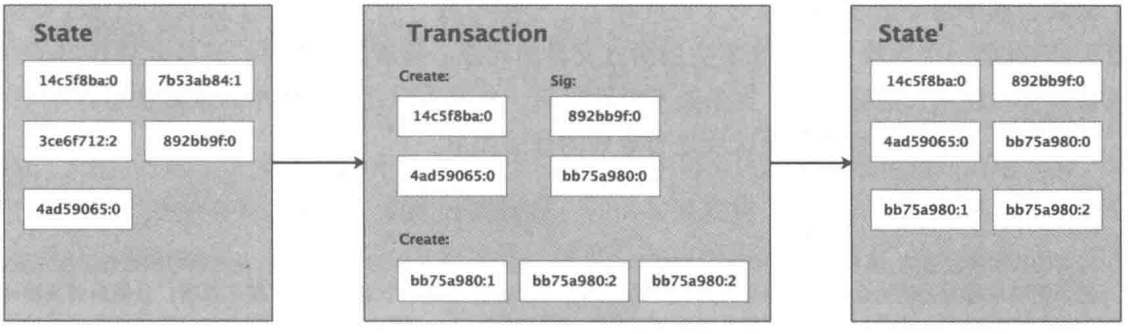


图1

但是，

```
APPLY({Alice:$50,Bob:$50},"send $70 from Alice to Bob")=ERROR
```

比特币系统的状态（State）是所有已经被铸造并且没有被花费［技术上称为“未花费的交易输出”（Unspent Transaction Outputs）或UTXO］的比特币集合。每个UTXO都有一个面值和一位所有者（由大小为20 Byte的本质上为密码学公钥的地址定义[①]）。一笔交易包含一个或多个输入以及一个或多个输出。其中，每个输入包含一个对现有UTXO的引用和由与所有者地址相对应的私钥所创建的密码学签名，而每个输出包含一个新的将要加入到状态中的UTXO。

在比特币系统中，状态转换函数APPLY(S,TX)->S′大体上定义如下：

1. 对交易中的每个输入：

·如果引用的UTXO不存在于状态S中，则返回错误提示；

·如果提供的签名与UTXO所有者的签名不一致，则返回错误提示。

2. 如果所有的输入UTXO的面值总额小于所有的输出UTXO的面值总额，则返回错误提示。

3. 返回S（新状态S′），S中移除了所有的输入UTXO，同时增加了所有的输出UTXO。

步骤1的第一部分是为了防止交易的发送者花费不存在的比特币，第二部分是为了防止交易的发送者花费其他人的比特币，同时确保价值守恒。为了将其应用于实际支付，假设A想给B发送11.7 BTC。首先，A会查看自身拥有的有效的UTXO集合，并确保其加起来至少有11.7 BTC。事实上，A不可能正好有11.7 BTC。假设他能得到的最小数额的比特币为6 + 4 + 2=12。那么，他可以创建一笔有3个输入和2个输出的交易。第一个输出为11.7 BTC，并附带B的比特币地址（表示所有者为B）；第二个输出为0.3 BTC的“零钱”，所有者为A。

■ 挖　矿

如果存在可信任的中心化服务，那么这一系统很容易实现。将上述功能进行准确编码非常简单。然而，想把比特币系统搭建成去中心化的货币系统，为了确保每个人都同意交易的顺序，需要将状态转换系统与共识系统结合。比特币的去中心化共识进程要求网络中的节点不断地尝试创建包含众多交易的区块（Block）。网络被设计为大约每10分钟产生一个区块，其中每个区块均包含一个时间戳、一个随机数、一个对上一个区块的引用（即哈希），以及前一个区块生成以来发生的所有交易的列表。随着时间推移，这样就创建出了一条持续且不断增长的区块链。这条链不断地更新，从而表示比特币账本的最新状态。

依照这一范式，检查一个区块是否有效的算法如下：

---

① 聪明的读者会注意到，事实上，比特币地址是椭圆曲线公钥的哈希，而非公钥本身。然而，从密码学术语的角度来说，把公钥哈希称为公钥完全合理。这是因为比特币密码学可以被认为是一个定制的数字签名算法，公钥由椭圆曲线公钥的哈希组成，签名由与椭圆曲线签名连接的椭圆曲线公钥组成，而验证算法包含用作为公钥的椭圆曲线公钥哈希来检查签名内的椭圆曲线公钥，以及用椭圆曲线公钥来验证椭圆曲线签名两个步骤。

1. 检查区块引用的上一个区块是否存在且有效。

2. 检查区块的时间戳是否晚于先前区块的时间戳[①]，而且比未来早2小时。

3. 检查区块的工作量证明是否有效。

4. 将上一个区块的最终状态赋予`S[0]`。

5. 假设`TX`是包含n笔交易的区块交易列表。对于满足i=0, 1, …, n – 1的所有i，令`S[i+1]=APPLY(S[i],TX[i])`。如果任何一笔交易i在状态转换中出现错误提示，退出并返回`false`。

6. 返回`true`，并将状态`S[n]`作为这一区块的最终状态。

本质上，区块中的每一笔交易必须提供一个有效的状态转换。需要注意的是，状态并不是编码到区块中的，它纯粹是一个被验证节点记住的抽象概念。任意区块都可以从创世状态开始，按序添加每一个区块内的每一笔交易，计算出当前的状态。此外，请注意矿工将交易打包进区块的顺序。假设一个区块中有A、B两笔交易，且B花费的是A创建的UTXO：如果A在B之前，那么这个区块是有效的；否则，这个区块是无效的。

在区块验证算法中，最有意思的部分是“工作量证明”概念，即对每个区块进行SHA256哈希处理，并将得到的哈希值看作长度为256 bit的数值。该数值必须小于不断动态调整的目标数值，本白皮书写作时的目标数值大约是2^{190}。工作量证明的目的是使区块的创建变得困难，从而阻止“女巫”攻击者恶意重新生成区块链。因为SHA256是完全不可预测的伪随机函数，创建有效区块的唯一方法就是简单地不断试错，不断地增加随机数的数值，查看新的哈希数值是否小于目标数值。

当前的目标数值是2^{192}，意味着平均需要尝试2^{64}次。一般而言，比特币网络每隔2016个区块重新设定目标数值，从而保证平均每10分钟就会有一个网络中的节点生成区块。为了对矿工的计算工作进行奖励，每一个成功生成区块的矿工都有权在区块中包含一笔凭空发送给自己25 BTC的交易。另外，如果交易的输入的总面值大于输出，差额部分就作为“交易费用”付给矿工。顺带提一下，奖励矿工是比特币唯一的发行机制，创世状态中并没有包含比特币。

为了更好地理解挖矿的目的，不妨分析一下比特币网络出现恶意攻击者时会发生什么。因为比特币的底层密码学是非常安全的，所以攻击者会选择攻击没有被密码学直接保护的部分——交易顺序。攻击者的策略如下，非常简单。

1. 向卖家发送100 BTC以购买商品（尤其是可以快速送达的数字商品）。

2. 等待商品送达。

3. 创建另一笔交易，将相同的100 BTC发送给自己。

4. 尝试让比特币网络相信：发送给自己的交易是最先发出的。

一旦步骤1发生，几分钟后矿工就会把这笔交易打包到区块。假定这是第270000个区块，大约1小时后，此区块后面将会有5个区块，其中每个区块都间接地指向这笔交易，从而“确认”这笔交易。这时，卖家收到货款，并向买家发货。因为假设这是数字商品，攻击者可以即时收货。现在，攻击者创建另一笔交易，将相同的100 BTC发送给自己。如果

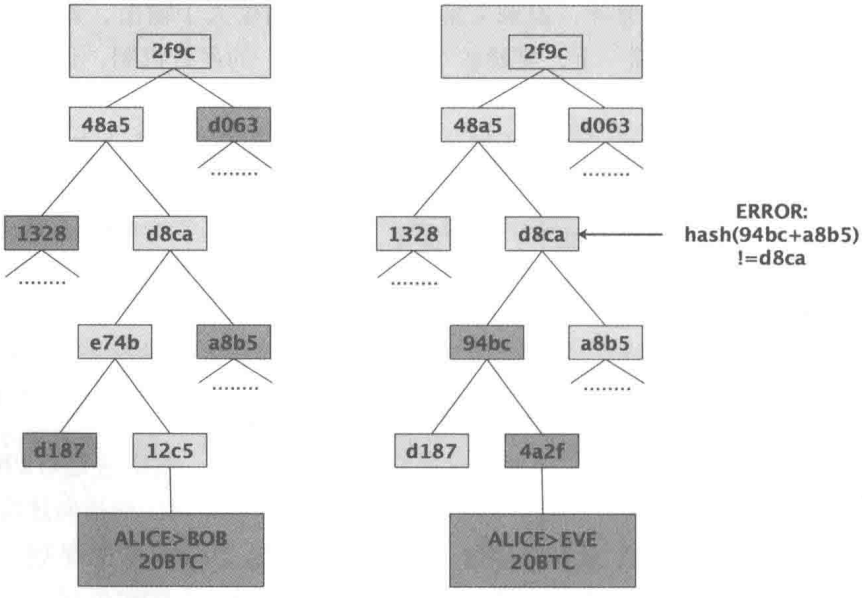
① 在技术实现中，是前11个区块的中值。

攻击者只是向全网广播这一消息，那么这一笔交易不会被处理。因为矿工会运行状态转换函数APPLY(S,TX)，然后发现这笔交易要花费的是已经不在状态中的UTXO。所以，攻击者会对区块链进行“分叉”，将第269999个区块作为父区块重新生成另一版本的第270000个区块，并在此区块中用新的交易取代旧的交易。因为区块数据是不同的，这一做法需要重新进行工作量证明。此外，因为攻击者生成的新的第270000个区块有不同的哈希，所以原来的第270001～270005个区块都不指向它。由此，原有的区块链和攻击者的新区块是完全分离的。依照比特币区块链的规则，发生区块链分叉时，链条最长（即有最多算力支撑）的分支将被认为是诚实的区块链。因此，合法的矿工将会沿着原有的第270005个区块后进行挖矿，只有攻击者一人在新的第270000个区块后挖矿。为了使得自身的区块链成为最长链，攻击者需要拥有比除自身以外的全网更多的算力来追赶（即“51%攻击”）。

■ 默克尔树

比特币的一个很重要的可扩展特性是，它的区块存储在多层次的数据结构中。一个区块的哈希实际上只是区块头的哈希。区块头是一段长度约为200 Byte的数据，里面包含时间戳、随机数、上个区块哈希和存储了所有的区块交易的默克尔树的根哈希。

默克尔树是一种二叉树，由一组叶节点、一组中间节点和一个根节点构成（图2）。其中，最底下的叶节点数量众多，节点内包含底层数据；而每个中间节点是它的2个子节点的哈希；根节点也由它的2个子节点的哈希生成，代表默克尔树的顶部。默克尔树的用途是使区块数据可以零散地传送：节点可以从一个来源下载区块头，然后从另一个来源下载与其有关的树的其他部分，但依然能够确认所有的数据都是正确的。这个方法之所以奏效是因为哈希是向上扩散的。如果一个恶意的用户尝试在树的底部替换一笔伪造的交易，其



左：仅提供默克尔树上的少量节点，就足以证明分支的合法性
右：对于默克尔树的任何部分进行改变的尝试，最终都会导致链上某处的不一致

图2

所引起的改动将导致树的上层及更上层节点的变动，最终导致根节点以及区块哈希的变动。这样，协议就会将其登记为一个完全不同的区块（几乎可以肯定是带有不正确的工作量证明的）。

默克尔树协议对比特币的长期持续性而言至关重要。截至2014年4月，比特币网络中的一个“全节点”——存储和处理所有区块数据的节点——需要占用15 GB的内存空间，并且还在以每个月超过1 GB的速度增长。目前，这一存储空间对台式计算机来说尚可接受，但是手机已经负载不了如此庞大的数据量了。不难想象，未来只有商业机构和爱好者才会充当完整节点。简化支付验证（SPV）协议允许另一种节点的存在，这种节点被称为“轻节点”。轻节点下载区块头，通过区块头来确认工作量证明，然后只下载与自身交易相关的默克尔树分支。这使得轻节点只要下载整条区块链的一小部分，就可以安全地确认任何一笔比特币交易的状态和账户的当前余额。

■ 其他区块链应用

将区块链思想应用到其他领域的想法早已有之。2005年，尼克·萨博（Nick Szabo）提出“用所有权为财产冠名”的概念，并描述了复制型数据库技术的发展如何将基于区块链的系统应用于土地所有权名录存储，以及创建包含诸如房产权、违法侵占和乔治亚州土地税等概念的详细框架。不幸的是，那时还没有实用的复制型数据库系统，所以这一协议并没有被付诸实践。不过，在2009年，即比特币的去中心化共识诞生以后，许多区块链应用开始快速出现。

1. 域名币（Namecoin）。域名币创建于2010年，是一个去中心化的域名注册数据库。在诸如Tor、BitMessage和比特币这样的去中心化协议中，都需要辨别账户的方法，才能够与用户进行交互。但是，在所有的现存的解决方案中，仅有的可用身份标识是类似于`1LW79wp5ZBqaHW1jL5TciBCrhQYtHagUWy`这样的伪随机哈希。理想情况下，用户会希望拥有一个带有类似于“george”这样的名称的账户。问题是，如果有人可以创建“george”账户，那么其他人同样也可以创建“george”账户来假扮他人。唯一的解决方案是使用先申请原则，只有第一个用户可以成功注册，后面的用户不能再次注册同一个账户。这一问题通过比特币共识协议就可以轻松解决。域名币是利用区块链来实现域名注册系统的最早且最成功的案例。

2. 彩色币（Colored Coins）。彩色币主要发挥类似于协议的功能，为用户在比特币区块链上创建属于自己的数字货币；或者，从更重要的单一单元的货币角度出发，为各类数字代币提供服务。依照彩色币协议，人们可以通过为某一特定的比特币UTXO指定颜色，从而发行新的货币。该协议递归地将其他UTXO的颜色定义为与交易输入UTXO相同的颜色，从而允许用户保持只包含某一特定颜色的UTXO。并且，发送这些UTXO就像发送普通的比特币一样，用户可以通过回溯区块链来决定他们所收到的UTXO的颜色。

3. 衍生币（Metacoins）。衍生币的理念是基于比特币区块链来创建新的协议，利用比特币的交易来保存衍生币的交易，但是采用了不同的状态转换函数`APPLY'`。因为衍生币协议不能阻止无效的衍生币交易出现在比特币区块链上，所以增加了一个规则：如果

APPLY'(S,TX)返回错误提示，那么这一协议将默认APPLY'(S,TX)=S。这为创建那些可能因为过于先进而不能在比特币系统中实现的加密货币协议提供了一个简单的解决方法，而且开发成本极低，因为挖矿和网络的问题已经由比特币协议处理好了。

因此，大体来说，构建共识协议有两种方法：第一，建立一个独立的网络；第二，在比特币网络上搭建协议。虽然像域名币这样的应用使用第一种方法已经获得了成功，但是该方法的实施非常困难：每一个应用都需要创建独立的区块链，同时建立并测试所有的状态转换功能和网络代码。此外，我们预测去中心化共识技术的应用将会服从幂律分布，即大多数的应用规模实在太小，以至于根本没有必要搭建专有区块链。我们还注意到大量的去中心化应用，尤其是去中心化自治组织，需要进行应用间交互。

另一方面，基于比特币的方法存在一些缺点：这些方法没有继承比特币可以进行简化支付验证的特性。比特币可以实现简化支付验证，是因为比特币可以将区块链深度作为有效性代理。在某一时刻，一旦某一笔交易的祖先们距离现在足够远，就可以认为这些祖先交易是合法状态的一部分。与之相反，基于比特币区块链的衍生币协议不能强迫区块链拒绝包括不符合衍生币协议场景的交易。因此，一个安全的衍生币协议的简化支付验证需要后向扫描所有区块直至区块链的初始点，以确认某一交易是否有效。目前，所有基于比特币的衍生币协议的“轻”实施都依赖于可信任的服务器提供数据，这对旨在消除信任需要的加密货币而言，并不是最理想的结果。

■ 脚 本

即使不对比特币协议进行扩展，也能在一定程度上实现智能合约。比特币的UTXO不仅可以被多把公钥拥有，还可以被更加复杂的用基于栈的编程语言所编写的脚本拥有。在这一范式下，花费UTXO的交易必须提供满足脚本的数据。事实上，甚至基本的公钥所有权机制也是通过脚本实现的：脚本将椭圆曲线签名作为输入，然后验证交易和拥有这一UTXO的地址。如果验证成功，则返回1；否则返回0。在更加复杂的场景中，脚本还可以依不同的应用而定。例如，人们可以创建要求集齐指定的3把私钥中的2把才能进行交易验证的脚本（多重签名）。对公司账户、储蓄账户和某些第三方托管商业服务来说，这种脚本是非常有用的。脚本也能用来对解决计算难题的用户发送奖励。人们甚至可以创建诸如“如果你能够提供你已经发送一定数额的狗狗币给我的简化支付验证证明，那么这一比特币的UTXO就是你的”的脚本。从本质上来说，这一脚本就是在不同的加密货币间进行去中心化兑换。

然而，比特币的脚本语言存在一些严重的限制。

1. 缺少图灵完备性。尽管比特币脚本语言可以支持多种计算，但它并不能支持所有的计算。其最主要的缺陷就是缺少循环语句。比特币脚本语言不支持循环语句的目的是，避免交易验证时出现无限循环。理论上，对脚本程序员来说，这是可以克服的障碍，因为任何循环都可以用多次重复的if语句的方式来模拟，但是这样做对脚本空间是一种浪费。例如，实施一个可替代的椭圆曲线签名算法可能需要256轮重复的乘法，并且每一轮乘法都需要单独包含在代码内。

2. 价值盲视。UTXO脚本不能为账户的提现额度提供精细的控制。例如，预言机合约的一个强大应用是对冲合约。在该场景中，A和B各自向对冲合约发送价值1000美元的比特币。30天以后，脚本向A发送价值1000美元的比特币，向B发送剩余的比特币。虽然实现对冲合约需要一个预言机来决定一个比特币对应的美元价值，但是与现有的完全中心化的解决方案相比，这一机制已经在减少信任和基础设施方面有了巨大的进步。然而，因为UTXO是不可分割的，实现此合约唯一的方法就是非常低效地采用众多拥有不同面值的UTXO（如一个包含2^k个输入的UTXO，其中每个k的上限是30），并使预言机挑选出正确的UTXO发送给A和B。

3. 缺少状态。UTXO只有已花费和未花费两种状态。为此，在UTXO模型中，那些需要保存其他内部状态的多阶段合约或者脚本刚没法实现。这也使得多阶段期权合约、去中心化交易要约或者两阶段密码学提交协议（对确保计算奖励非常必要）的实现非常困难。这同样意味着，UTXO只能用于建立简单且一次性的合约，而无法建立诸如去中心化组织这样有着更加复杂的状态的合约，也难以实现衍生币协议。二元状态与价值盲视结合在一起意味着另一个重要的应用——提现限额——是不可能实现的。

4. 区块链盲视。UTXO看不到诸如随机数和上一个区块的哈希这样的区块链数据。这一缺陷剥夺了利用脚本语言实现极具价值的随机源的可能，进而严重限制了其在博彩等其他领域的应用。

至此，我们了解了3种在加密货币上建立高级应用的方法：建立一条新的区块链，在比特币区块链上使用脚本，以及在比特币区块链上建立衍生币协议。可以通过构建新的区块链来实现我们想要的任意特性，但这不仅需要时间，还要投入不少精力。脚本的使用方法非常容易实现以及标准化，但它的能力有限。衍生币协议尽管非常容易实现，但错误地牺牲了可扩展性。在以太坊中，我们希望建立一个同时兼具这3种范式优势的通用框架。

以太坊

以太坊旨在将脚本、竞争币以及链上衍生币协议的概念进行整合及改进，从而使得开发者能够创建任意基于共识的应用。这些应用兼具上述范式所提供的可扩展性、标准化、特性完备、易于开发和互操作性等优点。以太坊通过建立终极的抽象基础层——一条内置有图灵完备的编程语言的区块链——使得任何人都能够编写智能合约和去中心化应用，并在合约或应用中创建他们自由定义的所有权规则、交易方式和状态转换函数。域名币的主体框架只需要2行代码就可以实现，而诸如货币和声誉系统等其他协议只需要不到20行代码就可以实现。至于智能合约，这一包含价值并且只有满足特定条件时才能打开的加密箱子，也能在我们的平台上创建；此外，考虑到以太坊的图灵完备性、价值知晓、区块链知晓和状态存在所加成的优势，使得以太坊上的智能合约比比特币脚本所提供的智能合约要强大得多。

■ 以太坊账户

在以太坊中，状态是由被称为“账户”（每个账户有一个20 Byte的地址）的对象、在