WHITE PAPER
SMART CONTRACTS
BITCOIN POWERED
ROOTSTOCK PLATFORM
RSK

根链平台

基于比特币驱动的智能合约

白皮书

（第 9 版）

日期：2015 年 11 月 19 日

作者：Sergio DemianLerner

译者：黄世亮

日期：2016 年 9 月 2 日

目录

1.引言

2008 年中本聪革命性地创造了比特币这套支付系统。比特币包含了一个有限功能的“智能合约”设计，这一概念由尼克·萨博（Nick Szabo）在 1993 年提出。

自那以来，有大量的研究致力于创建新的数字加密货币以支持图灵完备的分布式程序。现在有一个有广泛有信心的、实用的、安全的和确定性的虚拟机可以达成这一目标。

我们相信新的应用有必要让比特币成为世界领先的数字加密货币，而加入智能合约功能是达成这一目标的关键。甚至这一个认识我们设计了根链，一个基于比特币的具有图灵完备的智能合约平台。我们也加入加强了比特币网络的其它特性，如更快的交易传输和更好的可扩展性，我们相信这些特性将会用于创建新的应用场景。

根链是由 QixCoin 进化而来的，QixCoin 是一个图灵完备的数字加密货币，在 2013 年由相同的团队设计的。根链可以提供一个改进性的即时支付体验。它目前能实现 300tps 的交易处理量，大多数交易可在 20 秒内完成确认。并且这是基于比特币的安全保证的，支持 SHA-256D 的联合挖矿算法。

根链是比特币的侧链。当有比特币转入根链区块链时，这些比特币将变成“根币”（RTC）。根币相当于存活在根链区块链上的比特币，并且它们可以随时转回比特币区块链，并且不需要添加额外的交易费（除了根链的转账交易手续费外）。根币是根链这支侧链的代币，用于支付给矿工的转账手续费和合约处理手续费。根币并没有创造新的数字货币：所有的根币都是来自比特币区块链里的比特币转化过来的。

根链加强了比特币的以下特性：

- 允许参建智能合约的图灵完备性的根链虚拟机（RVM）。
- 第一个交易确认时间降至平均 10 秒。
- 基于联合的门限签名方案实现的安全联合工作量证明挖矿机制。
- 嵌入式低延迟快速中继骨干网络到点对点的八卦网络。

- 双向锚定使用侧链（目前是一个联合锚定，全自动的比特币协议的锚定）

注："RSK"是指根链平台，具体是指"RSK 协议"（规范）和"RSK 参考节点"（参考实现），本地 RSK 货币是"根币"，"RTC"是根币的符号，就和"BTC"是指比特币这一种货币，"Bitcoin"指比特币协议一样。

2. 为什么说根链是比特币经济生态里的重要一部分？

2.1 比特币经济里利益相关者和其价值保护

根链平台的首要目标就是让比特币主要利益相关者获得回报，这和目前比特币系统的运行目的是一样的。
这一理念直接体现在根链的核心架构上，在比特币系统里，矿工使用工作量证明（POW）提供算力验证区块，行业主要企业（交易所，钱包供应商和支付处理供应商）组成一类社区成员承担创建和验证检查点，以及使用双挂勾签署赎回交易这类整合工作。

根链平台顶层有一个改进型的投票系统，由矿工、行业领袖、比特币/根链持有者和核心开发者做最后决策。
在下面的段落中，我们将描述这种激励机制如何发挥作用。

2.2 治理模型

社区的每个角色都有专门的技术为社区提供最好的服务：交易所和网页钱包提供安全的比特币存储，矿工负责大规模的挖矿保证用户的安全交易，区块链公司创造新的应用让梦想变成现实，核心开发人员提供专业技术应对技术挑战，节点维护人员提供基础设施和网络连接，最后用户是整个系统的核心，提供信任和流动性。
根链的治理模式是建立社区成员代表制，设立五个董事会席位。矿工使用算力拥有投票权（1 票），比特币和根链的用户使用权益证明（POS）拥有投票权（1 票），交易所和网页钱包组成联合拥有投票权（1 票），比特币和根链的核心开发者将拥有一个特殊的通道行驶投票权（1 票），最后还有一票提供给比特币社区非营利性机构，比如比特币基金会，这样可以代表更为广泛的经济生态圈。甚至以太坊基金会也可以拥有公共性质投票权，以代表以太坊社区成员。

2.3 保护比特币矿工投资

2016 年 8 月（译者注：实际上是在 7 月就完成了），由于区块奖励从 25 BTC 减少到 12.5BTC，比特币商的盈利利润率将下降到低于 50%。数以百万计比特币挖矿机硬件瞬间将变得过时了。同时，由于二代芯片(更快的计算速度和更低的能

耗)将在 2017 年之前完成开发和销售，而且这可能会覆盖到今天所有挖矿机市场，那当前几乎所有未更换硬件的比特币商将会看到他们业务的结束。而使用联合挖矿技术，根链就可以给矿工带来两种币的收益，并且增加的边际成本却为零。这将为这些比特币矿机商带来了机会并可以继续获得至少四年以上的业务。只要根链提供的额外收入能补偿减半后的收益差距，那这些比特币旧矿机商仍然能够继续挖矿。
由于减半会造成矿工收益减少，这将可能导致算力集中到挖矿成本更低的矿工手上，这会让比特币网络的更脆弱。从这个角度说，根链平台可以给矿工提供额外的收益从而在保护比特币的安全和价值上扮演关键角色。
同时在根链平台上还可以低成本地创建应用，矿工不单单可以保证收益，甚至还可以发展全新的业务机会。

2.4 安全的比特币/根链的双向锚定机制

比特币业内领导型企业将组合成一个联盟，将在比特币和根链这两个区块链之间的资金安全转移发挥基础性的作用。这些企业也会在处理两个区块链资金的流入和流出时获得手续费。

2.5 更低的比特币交易费和稳定的价值资产发布

目前的比特币持有者和潜在的用户都看到了比特币价格的波动性限制了比特币的某些应用（如：投资，全球支付网络），可以预见的是在区块奖励减半后，比特币转账交易费进一步增加将会进一步限制比特币的应用。
根链将提供一个解决方案使得交易转账几乎可以瞬间（20 秒）完成，并且可以使用锚定定货币的价值和锚定特定的商品来发行数字资产。将比特币扮演一个储备货币的角色，从而降低比特币在使用过程的价格波动性，这将使得比特币更有价值。

2.6 加固比特币的安全

当下一个比特币区块减半时（已经发生。——译者注）数以百万美元计挖矿设备将被低价出售，或私下出售或在网上公开出售。这将可能导致有人可以以很低的价格购买大量的矿机组成算力以发动 51%攻击。因为安全性的担忧，这可能影响比特币的价格。通过联合挖矿的形式，让矿工可以同时获得比特币和根链的区块奖励，这或许可以阻止比特币网络的算力下降。

3. 根链是一个低手续续的比特币支付网络

如果比特币区块无法通过 一个硬分叉来实现扩容，当下一个区块奖励减半时，对一些应用程序来说比特币交易手续费将变得太高。根链的区块可以容纳更多的交易，自然会提供更低的交易费服务。详见下一章的关于未来交易手续费的分析。

未来的比特币以及转账交易费是不确定的：目前大家争议的区块最大限制将会导致未来比特币交易费大增。下面的表格我们对未来的交易费做预测，基于合理的假设将根链和比特币区块上的交易费做对比。

参数	比特币	根链
在相同的安全性下的确认时间对比	10分钟	10秒
反转概率低于0.1%需要的最少确认时间	20分钟（两个区块）	30秒（3个区块）
每秒最多交易次数	3.3tps（按平均tx交易数据大小估算）	最初可达300tps，可扩展到1000tps
正常情况下用户平均交易成本	6美元， 估算依据： -区块1.5tps的交易频率	市场价格不可估计
矿工打包一个标准交易需要的成本	1美分， 估算依据： -使用快速中继网络 -UTXO在内存池 -每个tx处理时间1ms -区块奖励25.2BTC 5美分 估算依据： -使用标准中继网络	<1美分（估计） 估算依据： -没有专业的根链硬件矿机 -几乎没有根链交易 1美分（估计） -矿工装载区块需要10ms的处理时间
到2016年末的交易费	1.6美元 估算依据： -区块大小没有增加 -BTC/USD汇率没有变 -相同的安全等级 -3tps	1美分（估算） 估算依据： -3tps

必须要提示的是上面的计算交易费是基于比特币价格停留在目前大约 240 美元/BTC。如果未来价格上涨 10 倍，那交易费也会随之增加，这将使得比特币区块链转变成为一个类似银行间的清算系统，而不是一个支付网络。同样重要的是链下支付系统将会出现，这会提供更便宜的手续费，但这将会是一个中心化的网络，比特币去中心化的局面将被改变。
下表显示的是 2016 年最有可能的交易费情况，基于全网算力难度增加 以及比特币价格上涨：

前提	比特币矿工打包每笔tx的成本	根链矿工打包每笔tx的成本
比特币价格上涨10倍	16美元	2美分
通过硬分叉使TPS增加10倍	11美分	0.2美分
比特币价格和TPS同时上涨10倍	1.1美元	2美分

随关比特币交易转账手续费的增加，用户将会转入低手续费的支付平台，如根链。

4. 根链的使用案例

根链平台提供了图灵完备的智能合约，智能合约是在 1993 年由尼克·萨博提出的。同时根链的虚拟机向后兼容以太坊的虚拟机，这为根链平台上的开发者在比特币区块链上获益的同时也能够有机会在以太坊平台上获利。下面我们举例说明根链的智能合约可实现的功能案例。

4.1 微支付通道和中心辐射型网络

微支付通道允许两人构建一个安全的支付规则，并且不需要手续费来完成小额支付，但是只有一次支付机会，然后支付通道就要关闭。
中心辐射射型网络让用户可以无需相互信任直接使用支付通道来完成小额支付，也可能依靠一个最低信任的第三方来完成支付。通过根链可以构建中心辐射型支付网络，简单直接并且是标准的电子钱包支付方式。

4.2 点对点的分布式交易所

使用 TierNolan 协议在根链上可以构建合约完成点对点的交易所功能。自动匹配出售和求购信息也是非常容易建立。这就使得可以依托区块链技术构建一定去中心化的不需要第三方参与的数字加密资产交易所。

4.3 零售支付系统

根链可以让比特币成为全球的日用零售业务的支付方式。阻止比特币为零售业使用的原因是比特币的确认时间（为确保安全性，比特币转账一般要等待 10 到 60 分钟）。根链可以让用户获得比特币的安全性的同时只需要几秒钟的确认时间。商家不需要第三方网关就可以实现立即收到付款。为零售提供支付方案的另一个关键要素是每秒交易量（tps）。根链网络使用 DÉCOR+协议可以将比特币的每秒支付交易量达到 300tps（是 Paypal 的两倍）。

4.4 托管服务

根链可以创建智能托管服务，用户通过签属一笔交易来定义托管规则是否该被执行，这个过程被托管的资金甚至不会被任何其它方接触。

4.5 创造数字加密资产

在根链平台可以创造数字加密资产（或者竞争币），并且安全性依托于比特币网络。鉴于根链平台对在平台上创造合约所需要的燃料费用要求很柔性，任何人包括学生到银行和公司都可以利用根链平台创建自己的加密资产。

4.6 资产证券化

根链平台也可以基于原子资产来发布数字化证券，将原子资产证券化。包括商业房地产信托基金、股票、债券和其他资产（或未来价值）都可以利用根链来完成数字证券化。这个功能将可以为缺乏现代金融系统的发展中国家里的小企业提供运营和成长资金解决方案。

4.7 去中心化汇款

这个特殊的功能对发展中国家特别重要和特别适合，这些地方因为缺少银行体系也缺乏信用体系，因此人民只能通过支付高昂的手续费来向家人汇款。

4.8 IP 注册和保护

可以在根链平台上创建合约以证明某种“存在”，这可以允许个体或机构向世界证明特定的文件（或产权）真实存在，其安全性依托于比特币区块链。这个应用场景特别适合于拉丁美洲、非洲和亚洲等没有可靠的产权注册登记制度的地区。

4.9 投票系统

在根链平台上可以创建一个特殊的数字资产，用于提供极端安全和透明的选举，并且成本非常低。

4.10 微借贷系统

全球超过 50%的人口没有享受到现代金融系统的服务，这我们当今全球社会经济不平等的一个直接原因。根链平台可以搭建可扩展的微借贷系统，为发展中国家的 30 亿贫困居民提供信贷服务。

4.11 可追踪式供应链

根链平台上可以创建某种数字钱包用于追踪实物化的物品的位置和路径信息。这种特殊的合约对零售业、食品和医疗行业特别有用。和根链上的其他应用场景一样，它的安全性也是基于比特币区块链的，并且成本是非常低的。

4.12 在线网络信誉与数字身份

发展中国家主要问题之一是穷人缺乏信誉文档和身份信息。这种情况阻止了穷人拥有投票权，获得健康信息，获得刑事受害报告以及无法享受金融服务。根链平台可以使用安全的比特币区块链和极低的成本建立数字身份。

4.13 全球在线游戏货币

拥有众多游戏玩家的游戏是有其内存的经济体的，包括提供了特殊的货币。随着游戏的发展，游戏玩家获得的虚拟游戏币是有价值的，并且常常会在二级市场里出售。但通货膨胀、欺诈和网络偷盗都威胁着游戏里的经济安全。并且游戏公司保管用户的虚拟财产本身也要面临法律和安全风险。随着全球化的进展，已经虚拟游戏的发展，游戏玩家越来越对一个游戏里的游戏币不能被应用于其它游戏感到不适。根链平台可以解决这些问题，将比特币（选题的根币）整合进游戏，也可以使用根链平台上创建一个数字资产。根链支付系统非常快，游戏引擎也可以将根链用做游戏支付系统，为玩家和玩家或公司和玩家之间的虚拟资产交易提供支付方案。支付过程仅仅需要点击一个链接或扫描一个二维码，支付系统就可以完成标准和电子钱包支付，也可以用于游戏公司的佣金支付。

4.14 互联网赌博和市场预测

调整支付同时意味着调整支出。比特币赌博网站中本聪骰子提供了无需注册快速投注的赌博方式，它使用的是 0 确认的链上交易方式，但这种试对赌博网站来说风险很大。根链平台提供了同样的用户体验，但可以获得交易确认的安全性。

4.15 公平的游戏

使用智能合约，并结合加密协议可以构建如智能扑克一样的应用，根链平台可以构建一种无需信任的第三方参与的纸牌游戏。

这些只是使用基于比特币区块链做为底层技术的根链的几个应用例子。特别重要的是矿工通过联合挖矿运用根链上的智能合约可以获得利益。

5. 技术概述

根链平台的核心是结合了以下三个特性：

- 一个图灵完备且占用资源确定的虚拟机（智能合约）
- 双向锚定的侧链（提供比特币计价的交易）
- 一个动态混合联合挖矿/联邦的共识协议（为共识的安全性），和一个低延迟网络（快速支付）

5.1 图灵完备的虚拟机

根链的虚拟机是智能合约平台的核心。智能合约是由高比例的网络节点自动执行。智能合约可用于处理合约间的信息、创建资金交易和改变合约里的存储状态。虚拟机运算操作码兼容以太坊虚拟机，让以太坊的合约在根链上完美兼容。在第一个版本里，虚拟机是通过解释执行的。在下一个版本里，将计划通过动态重定向操作码以兼容使用 java 字节码的以太坊虚拟机，并且强化安全性和内存的限制，形成一个根链虚拟机新版本。这将给根链虚拟的执行性能接近本地代码。

有以下特性：

- 独立的虚拟机，但是和以太坊虚拟机兼容的操作码。
- 根链给以太坊的用户提供了让他们的项目可以运行在比特币网络上，以享有比特币网络的安全性。
- 新的 int32 算力操作码，以及更好的即时编译（计划中）提供了更高的性能。

5.2 侧链

侧链是一个独立的区块链，其代币通过通过支付证明的方式自动锚定另一条区块链的代币。两个代币使用双向锚定实现自由兑换，并且是自动的，不会产生价格折损。在根链平台，根币双向锚定比特币（更重要的是，一聪根币，即根币里的最小单位，是锚定一聪比特币的，聪是比特币的最小单位）。

在具体实践中，当比特币换成根币时，并没有比特币在两条区块链上转移，因为比特币区块链是无法验证另一条区块链的交易的。当交换发生时，交易的比特币是被锁定在比特币区块链上，同时另一部分根币在根链区块链上被释放。当根币需要兑换回比特币时，就是反过来，根币被锁定，而等额的比特币在比特币区块链上被解锁。

5.2.1 50%第三方信任制侧链

完全的信任制和无需第三方信任制的双向锚定都可以用于智能合约平台。但比特币区块链并不支持智能合约，也不支持具有扩展 SPV 证明功能的本地操作码，因此在根链上部分双向锚定的系统需要一个半信任的第三方（STTP）。单个半信任制的第三方并不能控制被锁定的比特币，只有所有的半信任制第三方联合起来才能解锁比特币。这些第三方执行暂时保管被锁定的比特币，以及解锁比特币，并且当根币在根链上锁定时向用户支付比特币。

在根链上保护锁定资金的半信任制第三方是联邦成员。这是因为联邦有动机完成资金保管：他们必须是社区值得尊敬的人，比如大学，而且他们也得有能力维护网络节点的安全。资金的锁定和解锁是通过安全的网络节点来执行的，排除了人为干预。因此联邦需要有审计节点软件安全性的能力，特别是对于比特币资金的解锁部分要保证正确性。为进一步保证安全性，我们计划设计防篡改的硬件设备来加强联邦的联合验证算法。

一旦比特币通过硬分叉的方式加入特别的操作码或可扩展验证的 SPV 证明，或者一旦新的系统被证明是安全和无需信任的，联邦角色和半信任制就不在是必须的了，届时根链团队将改进根链，设计成无需信任的系统。

5.3 动态联合挖矿/联邦（译者注：翻译可能不准确，原文 Dynamic Hybrid Merged mining/Federation）

我们认为工作量证明是唯一的低成本防止区块链被篡改的共识机制。其它共识机制都有不需要消耗真正的有价值的资源来挖矿的缺点，从而依赖于声誉，并

阻止了匿名参与挖矿。其他的共识机制也都要求新加入者信任部分已有的参与者，并找到已经经过验证确认的账本。
高算力的工作量证明是基于周期性暴块并且需要低孤块率，这要求矿工在全网找到新区块时就停止计算并且重新在新的区块链头部开始挖矿。这样会导致挖矿有时间差，或者说是网络需要中途切换而导致延迟。这种时间差降低了比特币挖矿效率，哪怕是只浪费了几毫秒。因此根链使用 DECOR+区块奖励共享方案，以减少竞争，并且允许矿工延时切换到根链的最佳区块。如果矿工在切换矿机算力时一个根链区块被挖到了，他们将获得一个完整的根链区块奖励。如果他们延迟了切换，并且还在旧区块链头部挖矿，他们就相当于创建了一个叔叔块（译者注：这里的叔叔块原文是 uncles，是因为出块时间太短，网络延迟而出现的分叉，类似于比特币里的孤块）并且获得区块奖励分享。这样在任何情况下矿工们挖矿都不会被全部孤块掉，因为 DÉCOR+会给叔叔块支付奖励，也会向符合 GHOST 规则的叔叔块的正常和保证区块链安全的区块发放奖励。从而推动比特币挖矿效率的最大化。
因为我们预计前期根链的算力会低于比特币全网算力的一半。这将有可能导致其余算力对根链发动 51%攻击 ，以展开双花攻击。为了防止这种攻击，根链的矿工使用工作量证明挖矿会包含一个联邦检查点（译者注：原文是 federated checkpoints）。联邦检查点由注册过的联邦成员和客户组成，共同签名以决定最佳的区块链状态。并且根链还有最后一个保留协议，当根链算力低于比特币全网算力的 5%时，将由联邦来创建区块。在默认情况下，当根链的算力超过比特币链上难度最大时的算力的 66%，并且平均区块手续费高于比特币区块奖励时，客户端将停止使用联邦检查点，
根链平台推出的同时会组建一个知名的并广受社区尊敬成员组建的联邦。每一个成员都是使用公钥来签署检查点方案。联邦可以增加或移除使用和嵌入投票系统的成员，不过这些行为将需要一个高比例的成员投票。
根链网络的联合挖矿会激励矿工前来创建根链区块。在根链还缺乏算力来联合挖矿时，联邦会为网络提供安全。

主要特性：

- 成熟的挖矿奖励。（译者注：翻译可能不准确，原文是：1-day maturity for mining reward.）
- 联邦成员检查点。
- 在过度期代码嵌入检查点。
- 对比特币矿工来说，联合挖矿不会带来任何损失（中间状态立即切换损失低于 0.1%，以及延迟切近 0%。）

5.4 快速支付和低延迟网络

根链旨在建立一个更好的支付网络。为了实现快速支付，已经开发了数个办法：

- 使用免费的竞争性区块链（例如 超级账本（Hyperledger），瑞波（Ripple），封闭环系统（closed-loop））

- 使用中心辐射型（hub-and-spoke）网络（比如比特币的闪电网络）
- 使用高工作量证明快速区块（译者注：翻译可能不准确，原文是：high POW block rates）

中心辐射型网络要新增加中心节点，并且需要一个全新的完整钱包客户端，这是一个完全不一样的支付模式。虽然这种形式可以很容易在根链上实现，但这不是一个本地的快速支付系统。根链符合 DECOR+和 FastBlock5 协议，这可以实现平均出块时间达到 10 秒，并且不会导致挖矿中心化，这是自由自主挖矿和激励政策。

主要特性：

- 平均 10 秒出块。
- 两级块传输（2SBP）协议。
- 推送丢失交易（PMT）协议。
- 最后竞争区块全网广播以阻止私藏挖矿（译者注：翻译可能不准确，原文是：selfish mining）和降低陈旧块率（译者注：翻译可能不准确，原文是：stale block rate）。
- 延迟交易包含启发式（DTI）。交易延迟 5 秒就允许加入最快的区块去确认，因为交易已经存在于每一个节点的内存池中。
- 使用新的网络命令来传播带有时间优先级的区块头部。
- 在区块头部信息广播后，立即使用新的网络命令传播区块交易哈希列表。
- 在启发式未确认区块（MUB）上挖矿。矿工可以使用 5 秒退回方式连在带有还未完成交易确认的区块头进行挖矿。（译者注：翻译可能不准确，原文是：Mining over block headers with unverified transactions with a 5 seconds fallback.）
- 没有交易的区块的区块头部信息会被标记（这里的交易是不包括 coinbase 奖励）
- 每个连接协议配备双优先信息流（2PSC）（译者注：翻译可能不准确，原文是：Two Prioritized Streams for each Connection protocol (2PSC).）新的信息传输层使用信息切片技术，这允许两个并行的会话使用不同的优先级。这就允许区块头部信息以更高的优先级会话发送，并且可以中断任何正在传输的低优先级会话的信息。
- 本地路由优化协议（LRO）。本地优化区块路由是基于对等优先级的。本地优化交易路由是基于对待优先级的。（译者注：翻译可能不准确，原文：Local Route Optimization Protocol (LRO).Local optimal block

routing based on peer priorities.Local optimal transaction routing based on peer priorities.）

- 使用 DECOR+协议在竞争区块间共享区块奖励。
- 使用 GHOST 协议为区块链加权（译者注：翻译可能不准确，原文： GHOST protocol for chain weighting.）

6. 根链和其他区块链特性对比

我们尝试将根链和其他区块链产品进行对比，我们会看到根链是一种不伤害去中心化的更好的技术选择，衡量去中心的标准是运行完整节点的成本。

项目	比特币(Bitcoin)	以太坊(Ethereum)	公证通（Factom）	合约币（Counterparty）	根链（Rootstock）
平均确认时间	10分钟	12秒（GHOST）	1分钟（Federated servers）	10分钟	10秒（DECOR+GHOST）
安全阈值（由于私自挖矿）	~30%	30%到50%之间	~30%	~30%	50%（DECOR+GHOST）
图灵完备的智能合约	不支持	支持	支持	计划支持	支持
为比特币增加价值	——	No	No	No	Yes（联合挖矿）
和比特币整合	——	No	覆盖协议（Overlay protocol）	覆盖协议（Overlay protocol）	侧链
基于概率的验证和防欺诈的扩展性（Scalability via Probabilistic Verification and fraud proofs）	No	No	No	No	Yes
轻量级客户端（SPV clients）	Yes	Yes	No	No	Yes
Block relay backbone	Yes	Yes	Yes	Yes	Yes
本地支持用户自定义访问结构（Native support for userdefined access structures）	Yes	No	Yes	No	Yes
本地支持用户自定义签名方案（Native support for userdefined signature schemes）	No	No	No	No	Yes
简单集成硬件钱包（Easy Hardware wallet Integration）	No	Yes	No	No	Yes
安全保障	SHA256D矿工	Ethash矿工	SHA256D矿工+联邦	SHA256D矿工	SHA256D联合挖矿矿工+联邦
秘密交易	No	通过合约实现（Via contract）	通过外挂程序实现	No	计划使用AppleCoin协议支持本地秘密交易（Native support Planned using AppeCoin protocol）
独立的交易ID	No（延展性）	Yes	No	No	Yes
交易容量（tps）	3到24	无限	无限	3到24	发布时为300
本地代币	BTC	ETH	FACTOID	XCP	通过双向锚定的BTC

7. 即时支付技术预览

比特币被发明后，以工作量证明为基础的加密货币就形成了一种降低出块时间的趋势。比特币是 10 分钟出块，莱特币是 2.5 分钟，然后狗狗币降低到了 1 分钟，夸克币（QuarkCoin）降到了 30 秒，以太坊则是 12 秒出块。每一个新的加密货币都将出块时间降低了一点，但很少有设计者知道这样做意味着什么。为了理解区块打包时间间隔对加密货币的稳定性和交易容量的影响，需要考虑多

个影响因素。首先，影响出块时间间隔最重要的影响因素是产生无效区块的数据（译者注：这里译为无效区块的原文是 stale block，从上下文来看应该指的是被孤立的区块）。另外两个因素主要影响区块产生速率的稳定：区块传播协议和区块从最高高度挖矿的矿工到下一下最高高度挖矿的矿工的传播时间。我们根链对这些影响因素做了小心谨慎的分析，并且进行了模拟运行以考察网络的性能，包括可用性和安全性。在这一章节里，我们将了解这些根链使用的新协议是如何降低无效区块率的。

7.1 DECOR+协议

在比特币里，如果有两个甚至多个矿工在同一区块高度上都挖到了新的区块，就会造成明确的利益冲突。这些相竞争的矿工们都希望将自己挖到的区块添加到最长链上去，但同时其他并没有挖到区块的矿工却完全不关心到底是哪个矿工的区块最终被采纳。不过所有其他诚实的矿工和用户本质上都是希望选择同一个区块的，因为这可以降低逆转的可能性。理想的解决方案是激励相竞争的矿工选择相同的 parent（译者注：这里的 parent 和前面的 uncle 类似，分叉叫 uncle，这里的 parent 则是指父亲块不分叉的方向。暂未找到合适的中文来翻译），DECOR+协议就提供了正确的经济激励办法，以促成矿工们不需要更进一步的协作就可使选择趋同。DECOR+协议是一个共享奖励策略，使用经济激励的办法解决选择冲突，可实现：

1.当所有参与的成员都获得相同的区块链状态信息时，冲突的解决结果是确定性的。
2.解决方案考虑所有矿工收入的最大化，包括相冲突的矿工和其余矿工。
3.解决冲突的时间可以忽略不计。

7.2 区块传输协议

比特币和以太坊区块链转发区块都是将区块头和交易信息一起打包的。显而易见的是，这种策略受区块传播延迟和带宽大小的影响非常大。比特币矿工使用快速中继网络（Fast Relay Network）可以部分解决这个问题：快速中继网络是一个中心化的骨干网络，可以将区块以压缩形态传播，这是需要由中心化用户来维护的。根链在快速中继网络的基础上植入网络协议，获得低延迟的网络拓扑结构，并且不需要中心化的维护。

7.3 双存储区块传输（2SBP）

根链区块的传播是两成两部分的：第一部分只广播区块头。第二部分是广播包含交易哈希列表的区块。使用 2SBP 协议可以使传播信道容量加倍，这让每一个区块可以存储更多的交易。当节点接收到了区块头和对应的交易哈希列表后，节点就会重组区块并完成完整验证。

7.4 推送丢失传输协议（PMT）

考虑到每一个节点都存储了交易的哈希，并且节点之间都会相互告之这些交易，而矿工也会将自己内存池里确信的丢失的交易立刻打包进区块。这就使得二次通信要求补充丢失的交易变得没有必要了。在节点要求重发被丢失的交易之前就发送这些交易是 2SBP 协议的第三个阶段。

7.5 延迟传输交易包探试（DTI）

矿工只会打包他在几秒种前已经收到的交易。这可以以很高概率来保证交易在区块被挖出前被矿工接收到。考虑到延迟的交易是矿工最喜欢的，因为这可以减少区块的验证时间，同时也降低了竞争区块的机会。在未确认区块试探挖矿（MUB）（译者注：“未确认区块试探挖矿”是一个专用名词，我翻译的可能不准确，原文是“Mining on Unverified Blocks Heuristic”）在网络上是有效的情况是，这种优化组合是不需要的。

7.6 区块头先行传播（IBHP）

当一个最新的区块的区块头被节点接收了，节点在转发区块头之前只会检验工作量证明工作和区块高度信息，而不需要检验交易和验证区块合法性。这就允许区块头信息可以提前 1 秒以内的时间在网络上广播。

7.7 双优先流连接协议（2PSC）

每个网络连接都包含两个不同优先级的双逻辑双向流。即使是在低优先级信息正在使用低优先级流来发送中，高优先级流也可以被立即用来发送区块头。

7.8 未确认区块试探挖矿（MUB）（译者注：翻译可能不准确，原文是“Mining on Unverified Blocks Heuristic (MUB)”）

节点可以在区块高度最高处继续挖一个空区块，即使是在一个固定的时间间隔内交易被丢失。在这个时间间隔之后，矿工们继续挖矿，而不会去管之前是挖的什么区块。这些空块降低了带宽和区块链存储功能的利用率，但模拟显示，如果使用 DBI，生产空块的数量，以及存储这些空块需要的空间，以及因此造成的交易容量下降，都是很低的。

7.9 本地路由优化协议（LRO）

降低无效区块的数量对减少矿工之间的传播延迟非常重要。根链网络使用动态优化以减少矿工之间的传播延迟，并且给予矿工之间的通信更高的优先级。换句话说，根链的对等网络中嵌入了快速传输网络，使用地理位置定位和优化本地路由来加强了 gossip 协议。矿工间传输区块的路径是一个关键路径，这对对等网络来说是极端重要的。在对等网络的关键路径中存在非挖矿节点会导致无效区块的增加。在关键路径上的非矿工节点（如终端用户和监控节点）只能对矿工起到微弱的匿名化作用。从本地节点开始决定创建关键路径，可以使用 LRO 协议来优化节点的优先级。该协议在根链的随机拓扑网络中嵌入了一个动态的有向无环图（DAC）（译者注：这里的“有向无环图”原文是“directed acyclic graph (DAC)”），这个 DAC 可连接最佳的矿工。

7.10 比特币挖矿网络资源再利用

一个中心化的挖矿网络，有着大型的矿池，是能比完全分布式挖矿拓扑网络要生产更少的无效区块。因此对于快速支付系统，基于 SHA-256D 算法的工作量证明的加密货币要比基于非 ASIC 算法的工作量证明的加密货币更有优势。

7.11 真实网络拓扑

比特币的设计是假定网络是近似于一个随机图，具有一个平均的出入度（译者注：这里的“出入度”对应的原文是“out-degree and in-degree”）。但这和真实情况是有很大的出入的，网络节点采用本地决策以避免出现物理位置上的地域集群（至少对外连接来说是这样）。这对区块传播来说并不是最好的拓扑结构。对区块传播来说最好的拓扑结构是给最顶端矿工（top-miners）更优质的资源，激励矿工们直接相互连接，或者使用更快的路由让区块在他们之间传播。同时一个矿工和矿工直接连续的骨干网也能帮助降低无效区块的数量。考虑到对比特币的攻击，目前这种方案已经有人提出用于增强比特币的防御能力。根链使用 LRO 算法建立一个稳定的动态矿工骨干网，这样避免了矿工和矿工之间的认证成本、保护隐私成本，和避免了泄漏 IP 地址和潜在的 DOS 攻击的风险。

7.12 工作量证明函数验证时间

SHA-256 算法是可以非常快速地验证，所以比特币的工作量证明时间几乎可以忽略。但不一样的是，一个 scrypt 算力的工作量证明机制就需要花费 3 到 30 毫秒来验证，具体多长时间要基于其所选择的参数（抗 GPU，或抗 ASIC）。为了保护网络免于垃圾交易和 Dos 攻击，每一个节点在将最新区块头转发前都需要验证工作量证明计算结果，结果是验证延迟的时间会被区块在矿工间的关键路径上传播的跌点（hops）数呈倍数放大。

7.13 客户端网络协议栈

一个节点接收到一个区块头后，为了降低全网无效区块的产生，最好的办法就是尽快转发。这意味着所有其他节点活动会暂停或停止。根链的设计允许立即中止低优先级的操作，并且建立重新接受（re-tries）。为了允许立即转发，客户端网络堆栈不阻止客户端交易验证程序或其它家务活动（译者注：这里的“家务活动”原文是“housekeeping activities”），比如对区块链的重组。这样根链的客户端就可以实现多线程和动态分配线程优先级，可以提高接收区块头的线程的优先级。

7.14 区块开销（译者注：翻译可能不准确，原文是“The Block Overhead”）

大多数加密货币的区块头体积都是非常小的（~100 字节），相较于整个区块来说区块头的大小并不会造成显著的开销。根链的区块头更大一些，但是区块头的开销对传播时间有显著的负面影响，因为低级别的 MTU 网络一般是 1500 字节，这大于区块头的大小。（译者注：这一句译的不通畅，我也没有搞清楚原文的因果关系，原文是：The Rootstock header is larger, but the block header overhead does have a noticeable negative impact on the propagation time, since low-level network MTU is generally 1500 bytes, which is above the block header size.）

7.15 仿真

我们使用离散事件仿真专门设计了一个模拟区块传播的系统，并且成功模拟了区块传播。这个模拟器模拟了一组顶部矿工（top-miners）之间的相互协作，每一个矿工都处在一个随机图中，并且他们之间的跃点（hop）距离是在网络中的节点距离的平均值附近。即使这种情况不是最坏的，因为这对于顶部矿工

（top-miners）间的良好相互连接是最有利的，我们假设矿工的表现不比平均水平差。这个模拟的事件是在一个位置上产生一个区块，并且将区块广播到其他矿工位置。模拟仿真结果显示了一个包含 5 个区块和 300TPS 的根链（目前块间隔为 10 秒）。仿真的关键结果是一个交易在 20.35 秒内被接受的概率是 99.98%（反转概率为 0.02%）。请注意这个反转概率是没有考虑可能删除这个交易的分叉，所以在实际情况中这个概率要低的多。

7.16 安全联合挖矿

联合挖矿是一种允许比特币矿工同时挖其他加密货币的技术，并且边际成本接近零。根链的挖矿设备和使用方法和挖比特币是一样的，这就可以让比特币矿工在挖比特币的同时挖根链。这意味着，因为根链会支付额外的交易手续费，这可以很好的激励联合挖矿。但同时也意味着使用 pump-and-dump（译者注：这个词在股市里是庄家坐庄拉高和出仓的意思），或者平行链（parallel chains）来攻击网络的成本要比攻击非联合挖矿加密货币的成本更低。根链在初始引导阶段为防止攻击采取了多种保护措施：

- 联邦检查点（Federated checkpoints）：根链客户预设由联邦成员签署的检查点。联邦将包括由交易所和其他高安全成员参与组建。节点使用联邦检查点防御 Sybil 攻击并通知用户。
- 挖矿铸币成熟期：每一个矿工挖出的币有一个 24 小时的成熟期，略高于比特币（译者注：比特币新挖出的币需要经过 100 个区块后才可以用，平均一个区块是 10 分钟，那比特币的成熟期是 1000 分钟，约 16.67 小时）。增加这个成熟期时间可以减少 pump-and-dump 攻击。
- 源代码嵌入检查点。

8. 交易的隐私

根链的交易隐私并不比比特币更强，也是依赖于代理名的。然后根链的虚拟机是图灵完备的，所以诸如 CoinJoin 和 AppeCoin 等匿名技术可以非常安全而且不需要第三方信任，就可以移植到根链上。

9. 安全

竞争币并没有广泛地使用和比特币联合挖矿的技术，因为在数字货币最开始的部署阶段大的比特币矿池很容易发动 51%攻击。根链使用联邦检查点来实现根链平台的初始部署，这样显著地降低了风险。同时根链将会采用不低于比特币全网算力 30%的算力来发布。根链基金会将监视网络的健康状况，并且会使用报警系统通知用户，以保护根链网络免受回滚的攻击。

10. 可扩展性

根链的应用场景可扩展性远超过目前的比特币。根链的支付交易数据体积只有标准比特币支付交易的五分之一，并且单个区块的交易承载量是比特币的 8 倍以上。同时根链还计划提供数个用户可选择的签名方案：椭圆曲线签名（ECDSA），Schnorr 和 Ed25519。最后一个的性能是比特币采用的椭圆曲线签名（ECDSA）的数倍。

根链平均消耗的带宽只相当于比特币的一半，因为根链区块不包括交易数据，而是只引用前面已经知道的交易。使用概率验证和欺诈证据（译者注：原文是 probabilistic verification and fraud proofs）后可进一步降低存储空间和占用带宽的需求。

10.1 概率验证和欺诈证据（Probabilistic Verification and Fraud Proofs）

运行一个完整节点的成本是数字货币中心化的关键因素。越高的成本，中心化程度越高。我们相信去中心化的重要性也意味着数字加密货币不能成一个全球性的支付网络。这两个目标是相矛盾的。比特币已经提供了一个高度去中心化的网络，因为区块大小限制为足够低，以保证任何个人用户都可以参与。这就使得根链可以作为侧链以在比特币的基础上提供更广泛的扩展性，而同时比特币作为基础网络可对抗中心化组织对数字货币的控制。

我们相信在第三方信任、网络节点信任和自我验证这三者之间是可以找到一个平衡点的，我们也邀请用户找到一个他们认为合适的平衡点。根链允许节点只存储和验证完整区块链的一个子链，以降低节点成本。这是通过概率验证和欺诈证据来实现的。概率验证是这样一种技术，它允许一个（或部分）节点随机选择区块来验证，并且在只要满足一些条件下直接接受剩下的其他区块，这些条件是：经过了一些时间；已经添加了一些已经确认的区块；网络的连通性是足够的；没有有效的欺诈证据被广播，和一些可选的权威检查点信息被广播。欺诈证据是区块被标记为“欺诈”。当一个节点接收到一个欺诈证据，会去检查在相同高度上是否有已经被接受（但没有被验证）的区块，如果有就去执行验证。如果被验证为无效区块，则在本地重组一个最佳的区块链。广播欺诈证据的成本是很高的，因为欺诈证据本身也需要工作量证明。一个节点接受一个验证过的欺诈证据以阻止节点作弊。如果有必要，节点将请求发送一个最原始的工作量证明工作，以阻止廉价的使用肉鸡 IPs 发动 Dos 攻击（译者注：这里的“使用肉鸡 IPs 发动 Dos 攻击”翻译可能不准确，原文是：“DoS using compromised IPs”）。而矿工（包括 POW 矿工和联邦成员）都必须运行完整节点，如果一个攻击者使用隐瞒区块数据（但广播区块头）并不会影响最佳链（best-chain），因为矿工会快速清除掉攻击者的区块。

11. 结论

根链代表了 4 年来区块链技术发展的顶级技术，它将实现数字加密货币经济生态圈里的货币和支付系统可编程特性，同时将扩展比特币（货币）的价值。

根链将赋与全球开发者创建私人的或企业的去中心化解决方案，并且运行在最安全的全球化的网络基础上，并且交易手续费保持非常低，足于适应足够广泛的需求。

根链将让比特币矿工能够参与智能合约市场，并且显著增加挖矿行业的价值，以及确保矿业长期可持续性。

根链将给矿工创建一个更广泛的基础，加强对比特币网络的安全。

根链有助于去中心化的发展，将创建一个即使支付并且廉价的金融系统，这让世界上 30 多亿还没有银行账户和现代金融服务的人受益。

RootStock Core Team