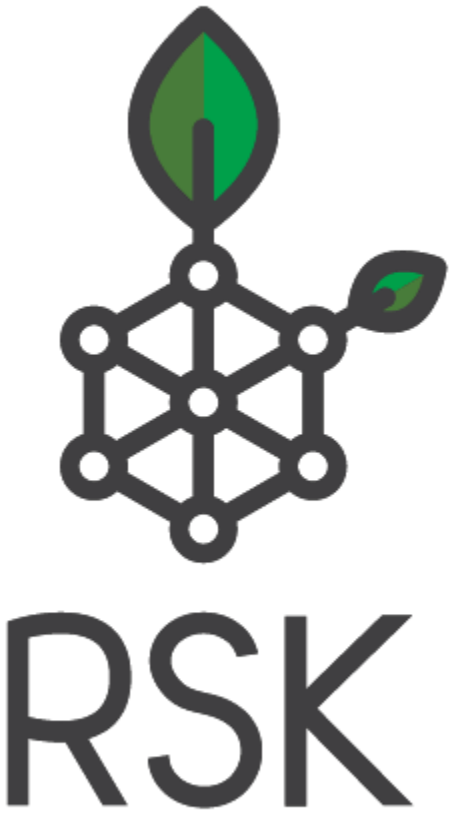

白皮书概述

修订：9
日期：2015 年 11 月 19 日
作者：Sergio Demian Lerner

简介

2008 年，Satoshi Nakamoto（中本聪）通过创建比特币彻底改变了支付方式。比特币包含了所谓“智能合约”的非常有限的实施，这是 1993 年由 Nick Szabo 引入的一个概念。

从那时起，许多研究致力于创建支持完整图灵完备分布式程序的新型加密货币。现在人们普遍相信，可以构建有用、安全和确定的虚拟机来实现这一目标。

我们认为，为了使比特币成为全球领先的加密货币，新的用例是必要的，增加智能合约能力是确保未来发展的关键。考虑到这一点，我们创建了智能合约平台 RSK，可将图灵完备虚拟机整合到比特币。它还为网络提供了其他增强功能，例如更快的交易处理和更好的可扩展性，我们也相信这些功能将支持新的使用情景。

RSK 是 QixCoin 的演变，QixCoin 是由同一开发团队于 2013 年创建的图灵完备加密货币。RSK 通过近乎即时的确认提供改进的支付体验。它目前达到每秒 300 次交易，并可在不到 20 秒的时间内确认大部分付款。而且，仍然基于比特币具有的相同安全保证，支持 SHA-256D 合并挖掘。

RSK 作为比特币侧链工作。当比特币转移到 RSK 区块链时，它们变成 “SmartBitcoins”（SBTC）。SmartBitcoins 相当于存在于 RSK 区块链中的比特币，它们可以随时转回比特币，无需额外费用（标准 RSK 交易费除外）。SBTC 是 RSK 侧链用于支付矿工进行交易和合约处理的基础货币。没有货币发行：所有 SBTC 都是来自比特币区块链的比特币。

RSK 在以下领域强化了比特币：

- 图灵完备的 RSK 虚拟机（RVM）允许智能合约
- 平均在 10 秒内首次确认交易
- 将 PoW 与基于备份阈值签名的联合挖掘相结合的安全合并挖掘
- 嵌入式低延迟快速中继骨干网成为点对点 gossip 网络。
- 使用侧链进行双向挂钩（目前是联合挂钩，全自动挂钩待比特币改进）

缩略词：“RSK” 是指 Rootstock（平台），相关术语是 “RSK 协议”（规范）和“RSK 参考节点”（参考实现），原生 RSK 货币是 “SmartBitcoin”，而 “SBTC” 是 SmartBitcoin 货币的符号，“BTC” 是指比特币货币，“比特币”是指比特币协议。

为什么 RSK 对比特币生态系统很重要？

比特币利益相关者的协调与价值保护

RSK 治理的主要目标是通过创建与其当前活动完全一致的奖励以调整比特币的主要利益相关者。

这种理念直接反映在其核心架构中，其中比特币矿工提供工作证明块验证所需的散列能力，行业领导者（交易所、钱包和支付处理器）集成了创建验证检查点并签署双向挂钩赎回交易的联合。

最重要的是，RSK 基于投票系统决定对其平台的改进，其中矿工、行业领导者、比特币/ RSK 持有者和核心开发人员做出最终决定。

在下面的段落中，我们描述了这种激励措施如何发挥作用。

治理模式

社区中的每个参与者都拥有为社区提供最佳服务的专业知识：交易所和网络钱包知道如何保护比特币储蓄，矿工知道如何实现大规模挖掘操作以确保用户的交易，Blockhain 公司在新用例方面进行创新，让梦想成真，核心开发人员拥有技术专长，知道如何应对即将到来的技术挑战，节点维护人员提供基础设施和网络连接，用户是系统的核心，提供信任和流动性。

RSK 治理模式旨在通过提供由 5 个席位组成的治理委员会来代表社区的所有参与者。矿工将能够以散列能力投票（1 票），比特币和 RSK 用户将投票通过股权证明（1 票），交易所和网络钱包将投票通过联盟（1 票），RSK 和比特币核心开发者将拥有一个特殊的门槛投票系统（1 票），最后一次投票将提供给一个非盈利的比特币机构，例如比特币基金会，它可以代表更广泛的生态系统。如果是以太坊社区的代表，也可以向以太坊基金会提供机构投票权。

保护比特币矿工的投资

2016 年 8 月比特币挖掘盈利率将降至 50% 以下，原因是 25 BTC 对 12.5 BTC 的区块奖励减少。数以亿计的挖掘硬件将立即过时。这可能包括当今市场上的所有挖掘机器，因为将在 2017 年之前开发和销售两代芯片（更快且功耗更低）。几乎所有尚未更换硬件的现有矿工都会发现他们的挖掘业务已经结束。RSK 合并的挖掘能力使其为这些矿工提供了至少继续营业四年的机会。由于比特币合并矿工可以以零边际成本开采两种硬币，只要 RSK 挖掘提供的额外收入弥补了盈利差距，矿工仍然可以开采比特币。

此外，减半的挖掘盈利能力下降将进一步集中于低成本矿工，这将增加比特币的网络漏洞。因此，RSK 还可以在促进广泛的盈利矿工基础方面发挥关键作用，从而提高比特币的安全性和价值。

此外，从今天开始，通过最低成本并为 RSK 创建应用程序，比特币矿工不仅可以保护他们的投资，还可以开发一个全新的商机。

保护比特币/ RSK 双向挂钩

领先的比特币公司将整合一个联盟，该联盟将发挥基本作用，确保比特币和 RSK 区块链之间的资金转移。作为交换，他们将从资金流入和流出之间的结算所产生的费用中获利。

降低比特币交易费用和稳定价值资产发行

目前的比特币持有者和潜在用户已经发现他们对货币系统的使用局限于某些用例（即投资、全球支付网络），主要是由于比特币价格波动，但由于交易费用可能增加，这种约束在未来下一个比特币减半时可能会恶化 。

RSK 通过提供几乎即时的交易验证（20 秒）和资产发行来提供解决方案，其价格与法定货币或其他稳定商品的价格挂钩。在保持比特币作为储备货币的同时降低交易中的波动风险会增加比特币的整体价值。

比特币安全加固

在下一个比特币奖励减半的情况下，过时的挖掘硬件将以数十亿美元的价格私下或在线销售。这将打开一个漏洞窗口，让攻击者可以用很少的钱购买大量的散列能力并执行 51% 的攻击。安全性的降低也可能影响硬币的感知价值。通过 RSK 合并挖掘提高比特币挖掘的盈利能力，比特币网络可能会阻止散列率直线下降。

RSK 作为低成本的 BTC 支付网络

如果比特币块的大小没有通过硬分叉增加，当下一个比特币奖励减半时，某些应用程序的比特币交易费可能会变得过高。由于 RSK 块可以容纳比比特币块更多的交易，RSK 自然会提供更低的费用。关于交易费用的未来情景分析，请参阅下一节。

比特币的未来及其交易费用尚不清楚：目前，关于最大块大小变化的争议性提案将对未来的交易费用产生很大影响。在下表中，我们尝试预测未来情景，并在增长和分叉的合理假设下比较 RSK 和比特币。

参数	比特币	RSK
在 Satoshi 等效下具有可比安全性的确认时间	10 分钟	10 秒
逆转概率最小确认时间为 0.1%	20 分钟（2 个块）	30 秒（3 个块）
最大每秒交易量	每秒 3.3 次交易 （假设平均尺寸为 tx）	发布时每秒 300 次交易 可扩展至每秒 1000 次交易
标准交易的当前用户平均成本	6 美分 假设： - 每秒 1.5 次交易	市场价格不可用
矿工的当前成本包括标准交易	1 美分 假设： - 使用快速中继网络 - UTXO 在内存中 - 每 tx 1 ms 处理时间 - 25.2 BTC 平均区块奖励 5 美分 假设： - 使用标准中继网络	< 1 美分（估计）假设： - 没有 RSK 特定的硬件切换。 - 几乎没有 RSK 交易 1 美分（估计） - 中断矿工以加载新标头会损失 10 毫秒的处理时间
截至 2016 年底的交易费用	1.6 美元假设： - 块大小不会增加 - BTC /美元汇率不变 - 相同的安全级别 - 每秒 3 次交易	1 美分（估计）假设： - 每秒 3 次交易

从上面的图表中需要注意的是，交易费用估算基于未经证实的事实，即 BTC 价格在 2016 年期间将保持在约 240 BTC/美元。如果在此期间价格上涨十倍，那么交易费也会增加，使得比特币区块链可用作银行间清算系统，而不是支付网络。同样值得注意的是，离线支付系统可能出现，提供更便宜的支付，但同时集中网络，并改变其分散的性质。

下表显示了 2016 年底可能出现的未来情景，假设网络散列难度与 BTC 价格上升率相同：

脚本	比特币 tx 对矿工的成本	RSK tx 对矿工的成本
比特币价格上涨 10 倍	16 美元	2 美分
TPS 通过硬分叉增加 10 倍	11 美分	0.2 美分
BTC 价格和 TPS 增加 10 倍	1.1 美元	2 美分

随着包含比特币交易的成本增加，用户将转向具有较低交易成本的平台，例如 RSK

RSK 用例

RSK 平台提供了由 Nick Szabo 在 1993 年提出的图灵完备智能合约。同时，RSK 的 VM 向后兼容以太坊 VM，因此 RSK 为开发以太坊的开发人员提供了从比特币区块链的稳健性中受益的机会。下面我们列出了可以通过 RSK 开发的潜在智能合约和用例列表。

微支付渠道和中心辐射网络

小额支付渠道允许双方进行安全的定期低价值支付，而无需为每笔付款支付费用，但渠道关闭时仅一次。

中心辐射网络允许相互不信任，且信任度最低的用户使用支付渠道间接地使用支付渠道进行低成本的一次性支付。RSK 允许中心辐射网络以最小的麻烦直接实现，并与标准电子钱包局部接口。

点对点分布式交换

使用 TierNolan 协议，RSK 支持充当点对点交换的合约。还可以轻松创建订单簿中的自动匹配。这允许分布式市场超过独立的区块链，在没有第三方的情况下交换加密资产。

零售支付系统

RSK 允许 BTC 在全球范围内用于每日零售交易。比特币零售使用的主要限制之一是其确认时间（从 10 分钟到 1 小时以确保不可逆转性）。RSK 允许消费者在几秒钟内通过确认，从而受益于比特币安全性。商家可以立即接受付款而无需第三方网关。任何平台在零售市场取得成功的另一个关键因素是能够支持大量的每秒交易量（tps）。RSK 网络使用 DÉCOR+ 协议，允许通过比特币区块链处理高达每秒 300 次交易（是 Paypal 的两倍）

托管服务

RSK 允许创建智能托管服务，其中 oracles 签署（或不签署）定义是否应该执行（或不执行）的交易，而不与托管下的资金进行任何联系。

加密资产创建

RSK 允许创建由比特币网络保护的加密资产（或 altcoin）。鉴于 RSK 可以灵活地为合约的燃料定价，这些应用程序（与所有其他应用程序一样）可以用于学生、银行和公司。

资产证券化

RSK 还允许创建由实际资产支持的数字代币。这可用于数字化商业化 REIT、股票、发行债务或任何其他资产（或未来的进展）。这一特定用例将为发展中国家的小企业提供独特的解决方案，传统金融市场现在可以满足营运资本或资本增长的需求。

分散汇款

这种特殊用例在发展中经济体中尤其重要，因为没有银行账户/无证件的人口必须支付高利贷费，以便向家人汇款以获取食物和住所。

知识产权保护/登记

RSK 允许开发能够复制所谓存在证明的合约，以允许个人和公司在比特币区块链安全性的任何给定时间点证明某个文件（或产权）的存在。由于土地登记机制不可靠，这个用例在拉丁美洲，非洲和亚洲的社会中尤其重要。

投票系统

作为加密资产的一个特例，RSK 允许创建数字投票，以最低成本实现极其安全和透明的选举。

小额贷款

超过 50% 的全球人口无法使用传统的金融体系。缺乏信用是导致我们全球社会现在面临的经济不平等的直接原因。RSK 允许开发可扩展的数字小额租赁合约，为世界上 30 亿最贫困的居民提供信贷。

供应链可追溯性

RSK 还允许创建数字钱包以（数字化）追溯和跟踪某个产品或批次的物理位置。这种合约在零售、食品和医疗保健等行业尤其有用。与所有其他用例一样，通过使用 RSK，可以以最低成本实现比特币区块链的安全性。

在线声誉和数字身份

发展中国家面临的主要问题之一是穷人缺乏文件和身份证。这可能导致穷人无法投票、获得医疗保健、报告犯罪/虐待和获得经济援助。RSK 允许以极低的成本创建与比特币区块链一样安全的数字全球注册表。

游戏内全球货币

许多多人游戏都有游戏内经济，包括私有货币。随着这些游戏的发展，虚拟货币变得像法定货币一样对用户有价值，并且通常在二级市场上交易。通货膨胀、作弊和在线盗窃成为用户关注的问题。此外，游戏公司可能面临用户虚拟货物寄售在法律和安全方面的障碍。随着世界变得全球化，虚拟游戏也将变得全球化，并且玩家会因为在一个游戏中赚取的钱不能轻易地花在另一个游戏中而感到不快。RSK 可以通过允许游戏接受 BTC（相当于 RSK 币）进行游戏内支付，或者创建受 RSK 保护的私人数字资产来解决这些问题。RSK 支付可以与低面额的闭环系统一样快，因此游戏引擎可以使用 RSK 作为游戏内购买系统，用于玩家到玩家的交易以及公司到玩家的虚拟产品。只需点击 URL 或扫描 QR 码，就可以使用标准玩家的外部电子钱包软件触发交易，还可以向游戏公司支付佣金。

互联网赌博和预测市场

快速付款也意味着快速支付。像 SatoshiDice 这样的比特币赌博网站已经设法使用 0 确认和链式交易提供无注册快速投注体验，但是对于赌博网站存在安全风险。RSK 允许通过近乎即时支付进行下注并进行区块确认。

公平游戏

通过整合智能合约，并结合精心研究的加密协议（如 Mental Poker），RSK 能够提供一个开放和公平的纸牌游戏平台，而无需受信任的第三方进行搜索。

这些只是可以使用底层比特币技术在 RSK 平台上开发和编程的许多其他示例中的几个示例。值得一提的是，比特币矿工（通过合并挖掘）将成为运营这些合约的人，并从运行这些合约所消耗的绝大部分燃料中受益。

技术概述

RSK 平台的核心是以下组合：

- 图灵完备的资源计算确定性虚拟机（用于智能合约）
- 双向挂钩比特币侧链（用于 BTC 计价交易）
- 动态混合合并挖掘/联盟共识协议（用于共识安全性）和低延迟网络（用于快速支付）。

图灵完备虚拟机

RSK 虚拟机（RVM）是智能合约平台的核心。智能合约由大部分网络节点并行执行。执行智能合约的结果可以是处理合约间消息，创建货币交易以及更改合约持久性存储器的状态。RVM 操作码级别与 EVM 兼容，允许以太坊合约在 RSK 上完美运行。在第一个版本中，VM 通过解释执行。对于下一个版本，计划通过动态地将 EVM 操作码重定向到类似 Java 的字节码的子集来模拟 EVM，并且安全强化和内存受限的类似 Java 的 VM 将成为新的 VM（RVM2）。这将使 RSK 代码执行具有接近本机代码的性能。

主要特点：

- 独立 VM，但在操作码级别与 EVM 兼容。
- RSK 为以太坊用户提供了使用比特币网络安全运行项目的可能性。
- 用于快速 int32 算法和更好的即时编译的新操作码 （计划好的），以获得更好的性能。

侧链

侧链是一个独立的区块链，其本国货币通过使用付款证明自动与另一个区块链货币的价值挂钩。当两种货币可以自由、自动地交换并且不进行价格谈判时，则存在双向挂钩。在 RSK 中，SmartBitcoin（SBTC）与 BTC 双向挂钩（更确切地说，RSK 中的最小账户单位 Rootoshi 与比特币的最小账户单位 Satoshi 挂钩）。

实际上，当 BTC 交换为 RTS 时，在单个交易中区块链之间没有“转移”货币，因为比特币无法验证另一个区块链上余额的真实性。当转移发生时，某些 BTC 被锁定在比特币中，并且相同数量的 SBTC 在 RSK 中被解锁。当 SBTC 需要转换回 BTC 时，SBTC 再次被锁定在 RSK 中，同样数量的 BTC 在比特币中被解锁。

半无需信任侧链

可以在两个平台上使用智能合约创建完全信任且无第三方的双向挂钩。但由于比特币当前不支持智能合约或本机操作码来验证外部 SPV 证明，因此 RSK 中的双向挂钩系统的一部分需要对一组半可信第三方（STTP）的信任。单个 STTP 不可控制锁定的 BTC，但只有大多数 STTP 能够释放 BTC 资金。STTP 临时存储锁定的 BTC，并解锁 BTC 以支付比特币用户 SBTC 被锁定在 RSK 中以被转移回比特币。

在 RSK 中，保护锁定资金的 STTP 正是联盟成员。这是因为联盟激励措施与 STTP 高度一致：它们必须是备受尊重的社区参与者，例如大学，并且他们还必须具备维护安全网络节点的技术能力。资金的锁定和解锁由这个安全的网络节点完成，无需任何人为干预。因此，成为联盟一部分的要求是能够审核为节点提供动力的软件的正确行为，特别是关于决定释放 BTC 资金的组件的正确性。我们计划创建防篡改硬件，以强制执行联盟验证算法，以进一步提高安全性。

一旦比特币添加特殊的操作码或可扩展性来验证 SPV 证明作为硬分叉，并且一旦证明新系统安全且无需信任，将不再需要作为 STTP 的联盟角色，并且 RSK 团队将实施更改以使 RSK 适应无需信任系统。

动态混合合并挖掘/联盟

我们相信 PoW 是唯一能够以低成本防止重写区块链历史记录的共识系统。所有其他不消耗宝贵的挖掘资源的共识系统都有这个缺点，并依赖声誉，并防止匿名参与挖掘。所有其他共识系统都要求新用户信任一组参与方以查找已分类帐的经过身份验证的检查点。

基于具有低孤儿浪费的周期性块的高速率 PoW 共识要求矿工在每次网络解决新块时停止其硬件矿工并重新启动它们以在新的标头中间状态下挖掘。这导致平均挖掘时间差或中间状态切换的网络延迟更大。这些差距降低了比特币挖掘的效率，即使它们只消耗了几毫秒。因此，RSK 使用 DECOR + 区块奖励分享方案来减少竞争并允许矿工延迟切换到 RSK 最佳区块。如果矿工每次发现 RSK 块时都切换硬件，他们就会争夺完整的 RSK 块奖励。如果他们切换迟延，并继续挖掘过去的块提示，他们会创建叔叔，并获得块奖励的份额。在这些情况中，他们都不是完全孤儿，因为 DECOR + 向叔叔支付奖励，而 GHOST 规则将叔叔视为正常的块并确保最佳链。因此，BTC 挖掘的效率最大化。

正如我们所预期的那样，RSK 散列能力将低于总 BTC 散列能力 50% 的时期。这将使网络容易受到 51% 攻击，其中剩余的散列能力优于现有的 RSK 散列能力以进行双倍花费。

为了防止这种情况，RSK 包括用于 PoW 挖掘块的联盟检查点。联盟检查点由联盟成员签署，客户可以使用大多数签名来更好地确定哪个是最佳链。此外，RSK 还有最后协议，如果挖掘能力低于比特币散列能力的 5%，联盟就能够创建签名块。默认情况下，如果 Roostock 散列能力超过最佳链中观察到的最大 BTC 散列难度的 66% 并且块中支付的费用高于或等于比特币块的平均奖励，客户端则将停止使用联盟检查点。

RSK 平台将与知名和社区受尊重的成员联合推出。每个成员都由检查点签名方案的公钥标识。联盟能够使用和嵌入投票系统添加或删除成员，尽管这些操作需要高比例的成员投票。

RSK 创始人的目标是 RSK 网络将激励合并挖掘。然而，RSK 对于合并挖掘短缺非常强大，因为联盟在短缺情况下会自动用于保护网络。

主要特点：

- 挖掘奖励的 1 天到期日。
- 联盟成员检查点
- 在引导期间对嵌入的检查点进行编码
- 合并挖掘预计比特币挖掘效率不会下降（即时中间状态切换小于 0.1%，后期切换小于 0%）

快速支付和低延迟网络

RSK 旨在成为更好的支付网络。为了实现快速支付，已经开发了几种解决方案：

- 使用无竞争块选择（例如，Hyperledger、Ripple、闭环系统）
- 使用中心辐射网络（例如比特币闪电网络）
- 使用高 PoW 块速率

中心辐射网络增加了新的集中化节点，并要求客户端钱包完全适应完全不同的新支付模式。虽然这样的替代方案可以很容易地在 RSK 上实现，但不是快速支付的本机系统。RSK 采用 DECOR + 和 FastBlock5 协议，允许达到 10 秒的平均块速率，不会为挖掘集中化创造激励，是自私挖掘和激励兼容。

主要特点：

- 10 秒块间隔
- 两阶段块传播（2SBP）协议
- 推送缺失交易（PMT）协议
- 最后竞争块的完全网络传播，以防止自私挖掘并降低过时的块速率。
- 延迟交易包含启发式（DTI）。每个矿工的块交易队列上的交易延迟 5 秒，以允许尽可能快的块验证，因为交易已经存在于网络每个节点的池中。
- 新的网络命令，用于传播具有时间关键优先级的块标头。
- 新的网络命令，用于在块标头传播后立即传播块交易散列列表。
- 在未验证块启发式（MUB）上挖掘。使用未验证的交易在块标头上进行挖掘，并使用 5 秒的回退。
- 块标头在没有交易时被标记（coinbase 除外）
- 每个连接协议的两个优先级流（2PSC）。具有消息切片的新消息传输层允许具有不同优先级的两个并行会话。这允许通过高优先级会话发送块标头，并中断通过低优先级会话传输的任何消息。

- 局部路由优化协议（LRO）。基于对等优先级的局部最优块路由。基于对等优先级的局部最优交易路由
- DECOR+ 竞争块之间的奖励共享协议。
- GHOST 链加权协议。

RSK 功能比较

我们尝试将 RSK 与其他区块链进行比较，并且我们表明 RSK 基本上提供了更好的技术选择而不会破坏分散化，其中分散化被测量为运行全节点实例成本的倒数。

项目	比特币	以太坊	Factom	对方	RSK
平均确认时间	10 分钟	12 秒（GHOST）	1 分钟（联盟服务器）	10 分钟	10 秒 (DECOR+GHOST)
安全门槛（由于自私挖掘）	~30%	在 30% 到 50% 之间	~30%	~30%	50% (DECOR+GHOST)
图灵完备的智能合约	否	是	是	已计划	是
为比特币增加价值	-	否	否	否	是（合并开采）
与比特币整合	-	否	叠加协议	叠加协议	侧链
通过概率验证和欺诈证明的可扩展性	否	否	否	否	是
SPV 客户	是	是	否	否	是
阻止中继骨干	是	否	是	是	是
对用户定义的访问结构的本机支持	是	否	是	否	是
对用户定义的签名方案的本机支持	否	否	否	否	是
Easy Hardware 钱包集成	否	是	否	否	是
安全保障	SHA256D 矿工	Ethash 矿工	SHA256D 矿工+联盟	SHA256D 矿工	SHA256D 合并矿工+联盟
保密交易	否	通过合约	通过外部程序	否	本机使用 AppeCoin 协议支持已计划
唯一交易 ID	否（malleab）	是	否	否	是
可扩展性［每秒交易次数］	3 到 24	无界	无界	3 到 24	300 在发布时
本机令牌	BTC	ETH	FACTOID	XCP	BTC 通过双向挂钩

即时付款技术预览

自从比特币创建以来，基于 PoW 块链的加密货币的间隔越来越小。首先是间隔 10 分钟的比特币，然后使用 2.5 间隔的 LiteCoin，然后是 1 分钟的 DogeCoin，30 秒的 QuarkCoin 和 12 秒的以太坊。每一种新的加密货币都会将其降低一点，但很少有设计师真正知道这样做的含义是什么。要了解块间隔如何影响加密货币网络的稳定性和能力，必须考虑几个因素。首先，影响短确认间隔可行性的最重要因素是产生的过时块的数量。另外两个因素主要影响过时的块速率：块传播协议和从顶级矿工到顶级矿工的块传播时间。对于 RSK，我们仔细分析了这些因素并运行模拟，以验证网络的性能，可用性和安全性。在本节中，我们将回顾 RSK 用于降低过时块速率的新协议。

DECOR +协议

在比特币中，当两个或更多矿工解决了同等高度的区块时，存在明显的利益冲突。每个竞争矿工都希望剩下的矿工选择他的区块作为最佳链条，而其余的矿工通常无所谓选择哪一个。然而，所有剩下的诚实的矿工和用户都希望他们都选择相同的区块提示，因为这会降低自然逆转概率。理想的解决方案是激励冲突中的矿工选择同一父级，DECOR +为融合选择设置正确的经济激励，而不需要矿工之间的进一步互动。DECOR +，一种鼓励经济上解决冲突的奖励分享策略，以便：

1. 当所有各方都能访问相同的块链状态信息时，确定性地解决冲突。
2. 所选择的决议是最大化所有矿工收入的决议，既适用于冲突中的矿工，也适用于其他矿工。
3. 解决冲突的时间可以忽略不计。

块传播协议

比特币和以太坊通过将块标头与块中包含的所有交易包装在块中来转发每个块。众所周知，这种策略虽然是最易于分析的，但众所周知在块传播延迟和带宽使用方面都表现不佳，而且这种情况加倍。比特币矿工使用快速中继网络部分解决了这个问题：这是一个集中式主干，以压缩形式中继块，并由单个用户维护。RSK 诞生时嵌入了网络协议的快速中继网络，低延迟属性来自网络拓扑，不需要集中化。

两级块传播（2SBP）

RSK 块分两个阶段发送：在第一阶段，只发送块标头。在第二阶段，发送块中包含的交易散列列表。使用 2SBP，信道容量加倍，允许在每个块中存储更多交易。在每个节点已经接收到块标头和与块标头相关联的交易散列列表之后，该节点尝试重构该块以便完全验证。

推送缺失交易协议（PMT）

由于每个节点存储由其对等体通告的交易散列值，因此矿工还立即发送他已知在每个对等池中丢失的块中包括的交易。这完全消除了第二次交互以请求附加交易的需要。在对等方询问之前发送丢失的交易是 2SBP 协议的第三阶段。

延迟交易包含启发式（DTI）

矿工仅包括在几秒钟之前收到的交易。这确保了在块被挖掘之前对等体已经已经接收到交易的高概率。请注意，延迟交易是矿工的最佳利益，因为它减少了块验证时间，因此降低了竞争块的机会。当未验证块启发式挖掘（MUB）在网络中生效时，不需要此优化。

立即块标头传播（IBHP）

当接收到最新块的块标头时，节点将在检查交易或块的有效性之前转发块标头，并且仅在前向时检查块 PoW 和高度。这允许报头在不到一秒的时间内通过网络传播。

每个连接协议的两个优先级流（2PSC）

每个网络连接包括两个具有两个不同优先级的逻辑双向流。即使在低优先级流上发送较低优先级消息，高优先级流也用于立即发送块标头。

未验证块启发式挖掘（MUB）

然后，在固定间隔期间，即使交易仍然丢失，节点也可以开始在标头顶部挖掘空块。在该间隔之后，他们恢复在以前挖掘的区块内继续挖掘。这些空块减少了有效带宽和块链存储使用，但模拟显示如果使用 DBI，则生成的空块数量，以及存储空块所需的空间和 TPS 的减少量都很低。

局部路由优化协议（LRO）

减少过时块的数量对于减少内部矿工传输延迟非常重要。RSK 网络经过动态优化，可以减少矿工间的延迟，并优先确定矿工之间的流量。换言之，RSK 在对等网络中嵌入快速中继网络，通过地理定位和最佳局部路由增强了 gossip 协议。内部挖掘机块转发路径是块传播的关键路径，因此对于对等网络而言极为重要。在关键路径中对等网络中存在的非矿工网络节点倾向于增加过时块的速率。关键路径中的非矿工节点（例如最终用户或监控节点）只能作为弱匿名化跳跃服务于矿工。为了仅从局部节点决策创建关键路径，使用 LRO 协议完成节点的优先级排序。该协议创建了有向无环图（DAC）的动态嵌入到 RSK 网络的随机拓扑中，其中该 DAC 最佳地连接矿工。

重新使用比特币挖掘网络

具有大型挖掘池的集中式挖掘网络往往比完整的分布式挖掘拓扑产生更少的状态块。因此，对于快速支付，基于 SHA-256D PoW 的加密币优于非 ASIC 友好的基于 PoW 的加密币。

网络的真实拓扑

比特币设计假设网络类似于随机图，具有一定的平均出度和度数。虽然这在现实中远非如此，但网络节点采取局部决策以避免形成地理集群（至少对于外向连接）。这不是帮助块传播的最佳拓扑。块传播的最佳拓扑结构是通过鼓励它们之间的直接连接或通过在它们之间更快地路由块来更好地服务于顶级矿工。直接的矿工到矿工骨干也可以帮助显著减少陈旧块的数量。已经建议比特币增加攻击的弹性。RSK 使用 LRO 启发式方法建立动态矿工的主干，而不会产生矿工到矿工认证、矿工隐私、IP 地址泄露以及可能相关的 DoS 攻击的成本。

PoW 功能验证时间

SHA-256 评估速度非常快，因此比特币 PoW 验证时间可以忽略不计。相反，scrypt PoW 可能需要 3 到 30 毫秒来评估，这取决于所选择的参数（ GPU 或 ASIC “电阻”）。为了保护网络免受垃圾邮件和 DoS 攻击，每个节点需要在再次转发块标头之前验证块 PoW，使得验证延迟乘以矿工之间的块关键路径中的跳数。

客户端网络堆栈

一旦节点收到块标头，它可以做的最好的减少网络中过时块创建的办法，就是尽快将其转发。这意味着应暂停或停止所有其他节点活动。RSK 设计允许立即取消低优先级操作并接受重试。为了允许立即转发，客户端网络堆栈不会在交易验证过程或其他内务活动（例如链重组）中阻止客户端。这是通过 RSK 客户端实现的，该客户端允许多线程并动态分配线程优先级以增强已接收块标头的线程。

块开销

大多数加密货币中的块标头很小（约 100 字节），因此标头大小（与整个块大小相比）不会造成很大的开销。RSK 标头较大，但是块标头开销确实对传播时间有明显的负面影响，因为低级网络 MTU 通常是 1500 字节，高于块标头大小。

模拟

我们使用专门为此目的构建的离散事件模拟来模拟块传播。模拟器模拟一小组顶级矿工之间的交互，每个顶级矿工在随机图中，其中它们之间的跳距离接近网络中节点之间的平均距离。即使这不是最糟糕的情况，因为顶级矿工的最佳利益是连接良好，我们假设矿工的表现并不

比平均水平差。模拟事件是在一个位置中创建块以及将块传播到每个其他矿工的位置。以下结果显示模拟 RSK 具有 5 个块间隔和每秒 300 次交易（当前块间隔为 10 秒）。关键的模拟结果是，在 20.35 秒流逝之前，交易被接受的概率为 99.98%（逆转概率为 0.02%）。请注意，这种反转概率没有考虑到替换叉也可能包含已删除的交易，因此在实践中它可能要低得多。

安全合并挖掘

合并挖掘是一种技术，允许比特币矿工同时开采其他加密货币，边际成本几乎为零。他们用于挖掘比特币的相同挖掘基础设施和设置被重新用于同时挖掘 RSK。这意味着，由于 RSK 支付额外的交易费用，合并挖掘的激励很高。但这也意味着使用抽水转储或并行链攻击网络的成本低于攻击非合并加密货币的成本。RSK 在初始引导阶段有几种防止攻击的保护措施：

- 联盟检查点：RSK 客户希望联盟成员签署检查点。联盟将包括参与平台成功的交流和其他高度安全的各方。节点使用联盟检查点来检测 Sybil 攻击并通知用户。
- 开采硬币成熟度：每个矿工币的成熟时间为 24 小时，略高于比特币。硬币成熟时间的增加减少了抽水转储攻击的激励。
- 检查点嵌入在源代码中

交易隐私

RSK 本身不提供比比特币更好的交易隐私，并且依赖于假名。然而，RSK 的 VM 是图灵完备的，因此可以安全地实现诸如 CoinJoin 或 AppeCoin 之类的匿名技术而无需第三方信任。

安全

合并挖掘并未被替代币广泛使用，因为在最初的加密货币引导期间，它允许大型比特币挖掘池通过 51% 攻击破坏新的加密货币。RSK 实现联盟检查点作为引导平台的安全方式，并显著降低此风险。此外，RSK 将以最小散列能力启动，相当于比特币散列能力的 30%。RSK Foundation 将监控网络运行状况，并将使用其警报系统通知用户并保护网络免受回滚攻击。

可扩展性

RSK 在目前的状态下可以扩展到比特币之外。RSK 支付需要标准比特币支付的五分之一，并且每个时间间隔的块有效负载比比特币高 8 倍。此外，RSK 还将提供多种用户可选择的签名方案：ECDSA、Schnorr 和 Ed25519。最后一个通常比比特币 ECDSA 曲线高几倍。

在所有条件相同的情况下，RSK 平均消耗的带宽比比特币少 50%，因为块不包含交易数据，而只包含对先前已知交易的引用。使用概率验证和欺诈证明可以进一步减少存储和带宽使用。

概率验证和欺诈证据

拥有一个完整节点的成本是影响加密货币集中程度的主要因素。成本越高，集中度越高。然而，我们认为分散的极端主义立场意味着加密货币不能成为全球支付网络。这两个目标是矛盾的。比特币已经提供了高度分散的网络，因为区块链大小限制足够低，以确保大多数个人用户可以参与。这使得 RSK 侧链可以提高比特币之外的可扩展性，同时将比特币网络作为防范货币控制集中化的保护。

我们认为可以在第三方信任、网络节点信任和自我验证之间进行权衡，并且我们邀请用户找到他们感到满意的比率。在 RSK 平台中，允许节点存储和验证整个块链的子集，以降低节点成本。这是通过概率验证和欺诈证明来完成的。概率验证是一种技术，其中（部分）节点随机选择它将验证哪些块，并且只要满足某些条件就接受剩余的块：一段时间已流逝，添加了一些确认块，网络连接是足够的，没有有效的防欺诈广播，并且可选地已经广播了一些权威检查点。欺诈证据是标记为“欺诈”的块。当节点收到欺诈证据时，它会检查是否已在局部接受（但未验证）具有相同高度的块，如果是，则验证该块。如果它无效，则相应地重新组织局部最佳链。广播欺诈性欺诈证据的成本很高，因为欺诈证据也带有工作证明。从对等方接收欺诈性欺诈证据的节点禁止欺骗对等方。如有必要，节点将向对等方请求初始工作证明，以防止廉价 DoS 使用受损 IP。矿工（包括 PoW 和联盟）必须是全节点，因此攻击者拒绝块数据（但是广播标头）不会影响最佳链，因为矿工将迅速丢弃攻击者块。

结论

RSK 代表了 4 年来区块链技术改进的顶点，它将使加密货币生态系统能够利用可编程货币和支付的最佳功能，同时增加比特币（货币）价值。

它将允许全球开发人员创建个人和企业分散式解决方案，这些解决方案在全球最安全的网络中运行，交易成本低，满足各种需求。

它将允许比特币矿工参与智能合约市场，为挖掘业增加重要价值并确保其长期可持续性。

它将有助于建立更广泛的矿工基地，加强比特币网络的安全性。

它将有助于开发分散、即时和廉价的金融体系，为我们这个世界上仍然没有银行账户和经济困难的三亿人创造包容性和机会。

RSK 核心团队