
RSK
ROOTSTOCK PLATFORM
BITCOIN POWERED
SMART CONTRACTS
WHITE PAPER

RSK

由比特币驱动的智能合约

白皮书
概述

修订：11
日期：2019 年 1 月 29 日
作者： Sergio Demian Lerner

简介

2008 年，Satoshi Nakamoto 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 推出的一个概念。

从那时起，一些加密货币已经推出了有状态的虚拟机，能够支持图灵完备的编程语言，利用智能合约的全部功能。已经开发了数千个与智能合约交互的分散式应用程序，称为 dApps，并且出现了新的用例。但是，每个新平台都使用新的高度推测和易失性原生代币。

自 2009 年 1 月 3 日成立以来，比特币已经巩固了自己作为最常用、最强大、最安全、最佳的价值储存，以及所有加密货币之间最安全的协议这一地位。但是大多数 dApp 都需要更复杂的规则，这些规则无法编码成比特币的类似谓词。这种限制引发了 2015 年 RSK 的诞生，以及 2018 年 1 月推出的 Mainnet。RSK 是一个平台，可以执行使用比特币作为本机资产的智能合约，从而有助于比特币作为全球领先的加密货币的价值，并将其扩展到 dApp 的所有潜在用例。RSK 是比特币的侧链，所以它有自己的网络和自己的区块链，但不是它自己的代币。与比特币相比，RSK 网络提供了增强功能，例如更快的事务处理和更好的可扩展性。

RSK 是两个平台的演变，QixCoin 和以太坊。QixCoin 是 2013 年由一些 RSK 创始人创建的图灵完备加密货币。QixCoin 引入了每次执行付费的概念，目前称为交易“气体”。但是，RSK 继承了以太网的几个关键概念，例如其账户格式，VM 和 web3 接口。因此，RSK 与以太坊编译器、工具和 dApp 高度兼容。

与比特币相比，RSK 提供了近乎即时确认的改进支付体验。然而，RSK 还基于支持 SHA-256D 合并挖掘的工作量证明、同样的共识协议和挖掘网络来保护比特币。截至 2019 年 1 月，RSK 拥有超过 40% 的比特币散列率，从而成为世界上最安全的智能合约平台，用于保护区块链的能源投入。

为了使比特币能够流入和流出 RSK ，RSK 与比特币有双向挂钩。当比特币转移到 RSK 区块链时，则变成“智能比特币”（ticker RBTC[1]）。智能比特币相当于存在于 RSK 区块链中的比特币，除了标准 RSK 和比特币交易费用外，它们可以随时转回比特币，无需额外费用。RBTC 是 RSK 区块链上使用的原生货币，用于向挖币者支付交易和合同处理费用。没有货币发行：所有 RBTC 都是来自比特币区块链的比特币。

RSK 目前在以下领域增强了比特币：

- 图灵完备的 RSK 虚拟机 (RVM) 允许智能合约，与以太坊的 VM (EVM) 高度兼容
- 平均在 30 秒内首次确认交易。
- 采用比特币合并挖掘。
- 双向挂钩侧链（目前是联盟挂钩）
- 使用 DECOR +协议防止自私挖掘

此外，RSK 社区强烈统一，遵循原始愿景，在未来的网络升级中添加以下功能：

[1]在本白皮书中，“RSK 协议”是指协议规范。“RSK 参考节点”是指参考实现。原生 RSK 货币是“智能比特币”。智能比特币的 “ticker”或符号是“RBTC”。“BTC”或“比特币”是指比特币的原生货币。“比特币”是指比特币协议。

- 存储租金
- 块传播优化
- 并行事务处理
- 事务压缩协议 (LTCP)，具有更高的可扩展性
- 支持基于 Java 字节码或 WAsm 的其他更高性能的 VM。
- 基于混合联盟/驱动链的挂钩

将来的功能描述为以下存储库中描述的 RSK 改进建议（RSKIP）
https://github.com/rsksmart/RSKIPs，以及 PoC 代码。

RSK 是一个社区驱动的项目。RSK Labs 是一家成立于 2015 年的公司，旨在开发 RSK 协议的参考实现，并且自 2015 年以来已向一些最著名的 RSK Core 开发人员支付工资。此外，RSK Labs 还在 www.rsk.co 网站上提供平台信息，并提供多种信息服务。

有用的入门资源

RSK Labs 网站：https://www.rsk.co/
RSK 统计数据：https://stats.rsk.co
RSK 探索：https://explorer.rsk.co/
RSK Faucet：https://faucet.rsk.co/
RSK 网络状态: https://twitter.com/RskSmartNetwork
RSK 费用比较：http://rskgasstation.info/

RSK 兼容软件钱包：

MyCrypto: https://mycrypto.com
Jaxx: https://jaxx.io/ https:/
iBitcome: /www.ibitcome.com/
Metamask: https://metamask.io/

RSK 兼容硬件钱包：

Ledger: https://www.ledger.com/
Trezor: https://trezor.io/
D'CENT: https://idcent.io/

为什么 RSK 对比特币生态系统非常重要？

在以下部分中，我们列举了 RSK 对比特币生态系统非常重要的几个原因。

比特币利益相关者的协调与价值保护

RSK 的目标之一是提供智能合约平台，使比特币生态系统及其社区的主要利益相关者受益。这种理念直接反映在其核心架构中，其中比特币挖币者提供保护 RSK 所需的散列能力，行业领先的公司整合了保存锁定在双向挂钩系统中资金密钥的联盟。RSK 治理模型旨在代表社

区的所有参与者，RBTC 利益相关者、挖币者、联盟成员以及 dApp 开发人员和最终用户。从长远来看，社区计划是在交易和区块中实现客观但不具约束力的信号机制，以便用户可以通过支付保证金发出信号，钱包应用程序和发送者可以通过标记交易发出信号，挖币者可以通过标记块发出信号，接收者可以通过标记账户来表明更加分散和民主的治理。

保护比特币挖币者投资

由于区块奖励从 12.5 BTC 减少到 6.25 BTC，因此在 2020 年 5 月，比特币挖掘盈利能力将下降。对于许多挖掘企业和个人而言，盈利能力的降低可能意味着结束，并且大量保有比特币的挖掘硬件将被停用。由于其合并挖掘的能力，RSK 为这些挖币者提供了继续经营更长时间的机会。由于比特币合并挖币者可以以零边际成本开采两个硬币，只要 RSK 挖掘提供的额外收入弥补了盈利差距，挖币者仍然可以开采比特币。

同样通过今天的合并挖掘，挖币者将支持新的未经批准的应用程序，这些应用程序在未来可能会提供全新的商机。

抵押比特币发行稳定价值资产

RSK 通过锁定比特币作为抵押，使资产发行的价格与法定货币或其他稳定商品的价格挂钩。稳定的资产实现较低的波动性，同时保持比特币作为储备货币可以提高整体比特币价值。大量比特币的锁定降低了流动性，因此有助于比特币价值的上升。然而最重要的是，RSK 上这些比特币烘焙的稳定代币将实现稳定的硬币小额支付，这使得目前缺乏传统金融系统的数十亿居民能够参与全球数字经济。

RSK 处于比特币侧链技术的最前沿

RSK Labs 正在探索、研究和实施对比特币未来任何其他侧链至关重要的关键概念。RSK 的成功将鼓励其他侧链开发人员遵循并从创建的高效合并挖掘基础架构、提出的驱动链操作码以及为 RSK Labs 安全创建多签名联盟而开发的技术中受益。通过开源软件，固件和硬件设计，RSK Labs 正在推进科学研究并改善整个加密货币生态系统的功能和安全性。

RSK 作为低成本比特币支付网络

目前，比特币交易平均成本为 24¢[2]，而 RSK 交易成本为 0.46¢[3]，低 50 倍。这是一个彻底的改进。但是，比特币费用通常会根据区块空间需求而上升或下降，我们预计对链码交易的需求也会增加。在几次尝试通过硬叉增加比特币的块大小失败之后，以及在一次性 Segwit 空间升级之后，比特币社区没有计划提高块大小。我们可以预期，对于涉及个人日常交易的大多数应用，比特币交易费用将变得过高。由于交易规模缩小，RSK 区块可以比比特币区块拥有更多交易，因此 RSK 自然会以相同的交易量提供更低的费用。在下表中，我们简要比较了比特币与 RSK。

[2] https://bitcoinfees.info/
[3] http://rskgasstation.info/

参数	比特币	RSK
平均块确认时间	10 分钟	30 秒（挖币者可以降低到 15 秒）
建议确认交换时间	30 分钟（3 个块）	使用当前合并挖掘散列值（40%）为 60 分钟（120 个块）。
最大每秒交易量	每秒 3.3 次交易 （假设平均规模为 tx）	每秒 10 次交易（对外交易，截至 2019 年 1 月） 每秒 20 次交易（内部交易）
当前平均交易成本	24¢	0.46¢

比特币交易的成本与块奖励的价值直接相关。向块添加事务会延迟其传播。传播所花费的每毫秒与块奖励成比例地支付，因为它降低了网络选择块的可能性。 集合协调技术（例如 Minisketch 库提供的 Bose-Chaudhuri-Hocquenghem 代码）如果实施到比特币中，可以减少这种依赖性。目前，如果比特币价格上涨，那么交易费也会上涨。我们认为，比特币将变得像银行间清算系统，而不是支付网络。同样值得注意的是，诸如 Lightning Network 之类的链外支付系统正在兴起，但这些网络可能会增加对渠道结算和充值的链上交易的需求，同时也会推高交易成本。随着成本的增加，用户将转向交易成本较低的平台。RSK 提供了以更低的成本进行比特币交易的绝佳机会。

为什么 RSK 对以太坊用户和开发人员非常重要？

增加您的 DApp 用户群

RSK 拥有一个独特的用户群，最初由 LATAM 的比特币用户组成。现在 RSK 在拉丁美洲和亚洲都在发展壮大。通过在以太坊和 RSK 中无缝部署兼容的 DApp，开发人员和公司可以扩展用户群，同时减少对任何特定区块链的依赖。目前还有几种联盟解决方案可以桥接以太坊和 RSK，并将代币从一个区块链转移到另一个区块链，因此相同的代币可以存在于两个区块链中。

促进 EVM / Web3 的标准化

以太坊社区创建了智能合约虚拟机 (EVM) 和分散应用程序与其交互的界面 (Web3)。通过采用这些标准，RSK 可以帮助开发人员将其应用程序迁移到 RSK，并重新利用大多数为以太坊开发的基础设施软件。但它也有助于标准化，提供统一的学习材料，减少学习另一种执行架构和编程语言的需要。同时，RSK 生态系统开发的所有工具也将可供 ETH 用户使用。

减少持续链叉风险

以太坊定期进行网络升级。最早宣布但仍在辩论的以太坊硬分叉之一是从工作证明共识向支付保证金证明的过渡。这是一项根本性的技术和经济变革，预计以太坊挖币者将面临此变革。新的链拆分将迫使开发人员在原始 PoW 链和新 PoS 链之间进行选择。关于新共识议定书的安全性和稳定性，仍然存在不确定性。如果失败，所有拥有以太的用户可能会受到经济影响，因此以太坊社区可能会对此更改提出质疑。除此之外，以太坊核心开发人员已实施并且将实施货币供应和工作证明算法的变更，这会损害平台的不变性和中立性。RSK 没有原生推测代

币，如果用户不同意社区支持的 RSK 网络升级，智能比特币总是可以移回比特币。因此，RSK 社区显示出极低的对抗水平，从而最大限度地降低了社区分裂的风险。另一方面，比特币有拒绝硬叉的传统。因此，RSK 在中长期提供了一个非常稳定的平台。

保护研发投资免受 0 天以太坊安全漏洞的影响

大多数区块链都会定期进行网络升级和频繁的软件更新。对于大多数区块链项目而言，技术尚处于试验阶段，且协议并不会一成不变。以太坊和 RSK 远未成熟。这意味着可以找到新的安全漏洞，因为此类漏洞曾在以太坊历史上被发现和利用。即使 RSK 拥有出色的安全记录，也并不是没有风险。但是，存在两个兼容的平台降低了由于平台的灾难性故障而导致专用于 DApp 开发的资源丢失的风险。特别考虑到所涉及的不同共识协议，同时发生故障的可能性要低得多。

通过将 DApps 移植到 RSK 增加交易处理量

RSK 技术上支持其他平台，因为有四个社区提案可以提供更高的链上可扩展性。第一种是由 RSKIP4 指定的并行交易处理，它使多核架构能够充分利用处理内核进行交易处理。这反过来允许增加块气体限制，从而实现更高的交易处理量。第二个是由 RSKIP53 指定的 LTCP，它可以压缩交易和聚合交易签名，例如可以使用相同数量的空间和处理资源处理更多交易。第三个是缩小链缩放，这是 LTCP 的扩展，以进一步减少签名空间和签名处理。第四个是改进的新虚拟机，它提供正在测试的 JIT 编译，其规范最终被提议为 RSKIP。

通过利用这些改进，RSK 可以支持更高的交易量和/或更低的交易成本。

通过将 DApps 移植到 RSK 降低交易成本

交易成本是许多 DApps 遇到的限制。由于 RSK 正准备通过上述扩展提案来增加链上处理能力，因此预计会降低交易费用。这将使得在以太坊上变得过于昂贵的用例成为可能。

降低币支付保证金和价值商店的贬值风险

许多 DApps 都需要使用加密货币。支付保证金是安全保证金，旨在提供选择服务的优先权。此外，一些 DApps 需要安全保证金作为抵御恶意行为的保险。然而，其他 DApps，例如 DAO 和众筹，要求资金长期锁定以进行归权。在所有这些情况下，原生加密货币的波动性降低了锁定币的动机。比特币作为一个平台表现出更大的弹性，并且作为一种价值存储的较低差异，品质由智能比特币继承。因此，RSK 可以更好地为这些应用提供服务。

RSK 用例

RSK 平台提供了由 Nick Szabo 在 1993 年提出的 “图灵完备”[4] 智能合约。与此同时，RSK 的虚拟机向后兼容以太坊虚拟机，因此 RSK 为开发以太坊的开发人员提供了从比特币货币的稳健性和 RSK 区块链的安全性中受益的机会。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。

小额支付渠道

小额支付渠道允许双方执行安全频繁且通常低价值的支付，而无需为每笔支付支付链上交易费用，但仅在渠道关闭时支付一次。这些应用程序将成为公平和包容性新金融系统的关键构建模块，它将为当前系统服务不足的数十亿用户提供替代方案。

第二层链外支付网络和状态信道网络

小额支付渠道为第二层链外支付网络提供了基础。第二层网络能够将支付从任何参与者路由到任何其他参与者，只要有足够的信道容量和低第三方信任。

第二层网络可以由节点的随机图实例化，也可以成为集线器和分支网络，其中少量高度互连的集线器通过大多数用户间支付。 状态通道网络使一组参与者能够执行即时创建的多方协议，例如游戏，这可能导致链路状态变化，例如代币传输，但延迟所有链上效应至信道关闭时止，前提是没有任何一方试图作弊。RSK 丰富的编程语言使所有这些第二层网络能够以最小的麻烦直接实现。

去中心化兑换 (DEXs)

去中心化兑换可以在没有第三方信任的情况下创建分散式代币和加密货币市场。RSK 支持所有变体的去中心化兑换，包括在线或链外订单，具有简单的订单匹配证明，从最简单的 TierNolan 协议 到基于 zk-SNARK 的更复杂的协议。

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 允许消费者在一分钟内通过付款确认，从而受益于比特币安全性。商家可以在不需要第三方网关的情况下几乎即时接受付款。RSK 还提供了更高的每秒交易量（tps），这是在零售市场取得成功所必需的。当交易量增加时，RSK 网络使用 DÉCOR+ 共识协议以防止挖掘集中化。

托管服务

RSK 允许创建智能托管服务，其中 oracles 可以签署一个交易，定义是否应该在没有 oracle 保管托管资金的情况下释放托管。

[4]尽管合同可能是图灵完备的，但由于使用通用语言为图灵完备指令集编写，因此虚拟机可用的资源有限。

加密资产创建

RSK 允许创建由比特币网络保护的加密资产（代币，替代币等）。这些资产可以是忠诚度积分，实用程序代币或安全代币。此外，代币可以是法定货币，也可以是备选法定货币。最终，它们可以由政府或中央银行创建，作为向所有公民提供低成本可编程资金的一种方式。

比特币支持的代币产品（BTO）

当比特币交换到新铸造的代币时，BTO 是加密资产创建的特例。该工具已广泛用于区块链众筹，如以太坊众筹。
在 RSK 的特定情况下，BTO 允许初创公司直接在比特币中接收资金，比特币是现存最安全和稳定的加密货币，同时在 RSK 区块链上创建由比特币散列率合并 RSK 保护的代币。使用 RSK 桥接服务可以使代币发布的整个过程变得无法信任。

资产证券化

RSK 支持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，在这些国家，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。RSK 支持以法定计价的代币，并利用现有的交易基础设施和加密资产的现金支付选项，可以以低得多的成本提供汇款。

知识产权保护/登记

RSK 支持开发提供存在证明（PoE）的合同。 PoE 使个人和公司能够通过比特币区块链的安全性在任何给定时间点证明某个文件（或产权）的存在。这个用例在拉丁美洲、非洲和亚洲的社会中可能特别重要，由于其身份和土地登记机制不可靠。

投票系统

RSK 可以创建数字投票，以最低成本实现极其安全和透明的选举。此外，它还可用于确保公司董事会或分散组织的透明投票流程。

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 可以开发可扩展的数字和可编程小额贷款合同，为世界上 30 亿最贫困的居民提供信贷。

供应链可追溯性

RSK 可以创建数字钱包，以跟踪和追踪（数字化）某个产品或批次的物理位置。这种合同在国际贸易以及零售、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 能够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机构。

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主要风险和用户关注的问题。此外，游戏公司可能因为在寄售中使用用户的虚拟货币面临法律和安全障碍。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（在等效智能比特币或 RBTC 中）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。第二层链外网络提供的 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虚拟给付。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 允许使用具有非零块确认的几乎即时支付进行投注。

公平博彩

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。

不可伪造代币（NFT）

NFT 是唯一的代币，可以链接到特定的财产、许可证、产品或服务。可以在 RSK 上轻松创建 NFT，允许从体育收藏品到游戏播放器功能或“皮肤”等多个行业的用例。

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）
- 基于通过定制 HSM 模块保护联盟的双向挂钩比特币侧链（用于 BTC 计价交换）。一旦 Drivechain 协议在比特币上实现，原计划就是转向混合驱动链机制。
- 抵御自私挖掘的基于合并挖掘的共识协议
- 低延迟块传播网络（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。智能合约由所有网络完整节点执行。执行智能合约的结果可以是处理合同间消息，创建货币交易以及更改合同持久性存储器的状态。RVM 与操作码级别的 EVM 兼容，允许以太坊合约在 RSK 上完美运行。目前，VM 通过解释执行。在未来的网络升级中，RSK 社区的目标是大幅提高 VM 性能。一种建议是通过动态地将 EVM 操作码重定向到类似 Java 的字节码的子集来模拟 EVM，并且安全加固和内存受限的类似 Java 的 VM 将成为新的 VM（RVM2）。 这可能会使 RSK 代码执行到接近原生代码的性能。

主要特点：

- 独立 VM，但在操作码级别与 EVM 高度兼容。
- 使用比特币网络的安全性运行以太坊 DApps。
- RSK 社区创建的众多 RSKIP（RSK 改进提案）中记录了性能改进管道。

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，智能比特币（RBTC）与 BTC 双向挂钩。

在实际操作中，当 BTC 交换为 RBTC 时，单个交易中的区块链之间没有“转移”货币。当发生转移时，某些 BTC 被锁定在比特币中，并且相同数量的 RBTC 在 RSK 中被解锁。当 RBTC 需要转换回 BTC 时，RBTC 再次被锁定在 RSK 中，同样数量的 BTC 在比特币中被解锁。

如果两个平台具有图灵完备智能合约，则可以创建完全信任最小化和第三方免费双向挂钩。但由于比特币当前不支持智能合约或原生操作码来验证外部 SPV 证明，因此 RSK 中的双向挂钩系统的一部分需要信任一组半信任的第三方（STTP），我们统称联盟。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。每个 STTP 都有一个密钥保护被锁定的 BTC，并且在接收来自 RSK 区块链的命令时，它解锁需要转移回比特币的 BTC。须

注意的是，如果用户将 BTC 传输到 RBTC 并返回，她通常不会收到由 UTXO 与原始 BTC 直接连接的比特币。因此，不要为特定用户锁定 RBTC，而是为整个 RSK 网络锁定 RBTC。
资金的锁定和解锁由联盟完成，无需任何人为干预。加入联盟的一项要求是能够审核为节点提供支持的软件之正确行为，特别是关于决定发放 BTC 资金的组件之正确性。RSK Labs 为 STTP 可以使用的硬件安全模块（HSM）开发了固件，以便为其私钥提供最大的安全性，并在将来能够实施事务验证协议以进一步提高安全性。

截至 2019 年 1 月，RSK 联盟由 15 位知名且高度安全的公证人组成。领先的区块链公司目前正在整合 RSK 联盟并参与自动协议以安全锁定比特币。作为其工作的交换，联邦成员将获得 RSK 产生的交易费的 1%，以支付硬件和维护费用。使用一个自动化过程来修改联盟的组成。每个联盟成员可以接受或拒绝组成变更。这个过程很少发生，由智能合约指挥，所以其对公众开放。该协议具有统一的强制延迟一周，直到激活更改。这允许用户将比特币转移回比特币网络，以防他们不信任新的联盟组成。

如果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，并且一旦新系统被证明是安全且无需信任，则不再需要作为 STTP 的联盟角色，并且 RSK 社区可以实现使 RSK 适应无需信任系统的更改。RSK 社区还提出了一个驱动链 BIP，它使挖币者能够参与固定挂钩中的比特币，并进一步减少对 STTP 所需的信任。

合并挖掘

Satoshi 共识，基于工作证明，是唯一一个阻止以低成本重写区块链历史的共识系统。学术界正在推进作为替代方案的支付保证金证明 的知识和研究，但目前 PoW 提供了最高级别的安全性。合并挖掘是一种技术，允许比特币挖币者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，当 RSK 以额外的交易费用奖励挖币者时，合并挖掘的激励变得很高。

我们已经确定了 RSK 合并挖掘增长的三个阶段：

- 自举阶段：合并挖掘低于比特币仇恨的 30%。
- 稳定阶段：合并挖掘是比特币散列率的 30% 到 60% 之间。
- 成熟阶段：合并挖掘高于比特币散列率的 60%。

RSK 已经过自举阶段，当时流氓合并挖币者可以低成本恢复 RSK 区块链。截至 2019 年 1 月，超过 40% 的比特币挖币者从事 RSK 合并挖掘。但由于 RSK 费用与比特币区块奖励相比仍然较低，因此双重花费攻击 RSK 的成本低于比特币。
RSK 有一些属性可以降低双重花费攻击的风险，例如长期挖币者奖励成熟度。RSK 实验室研究团队仍然已经开发了一些保护措施，以防止在项目的稳定和成熟阶段发生攻击：

- **签名的通知：**RSK 客户端可以使用公证人签名的通知。节点可以使用这些通知来检测 Sybil 攻击并通知用户。
- **透明的双重花费路径：**这是一种方法，其中所有 RSK 合并挖掘标签都增加了可用于检测比特币区块链中公开的自私 RSK 分叉的附加信息。自私叉证明为自动构建，且这些证明将呈现给 RSK 节点，这些节点将它们分布在网络上。证明强制节点进入“安全模式”，其中没有任何交易被宣告为已确认。安全模式可防止商家和交易所接受可

能会产生双重花费的付款。一旦经过验证的自私叉被 RSK 主链在累积的 PoW 中超越，网络就会恢复到正常状态。这种方法对任何 RSK 双重花费尝试都是一种威慑（恶意挖币者在挖掘自私叉时仍试图收集比特币奖励）。

一旦平台进入成熟阶段，我们估计 RSK 的安全性将足以支持全球金融包容性的经济。

主要特点：

- DECOR +共识协议
- 挖掘奖励的 1 天到期日。
- 合并挖掘预计比特币挖掘效率不会下降（中期后期转换）

快速支付和低延迟网络

RSK 已经启用了第二层链外支付网络，但与比特币相比，RSK 仍然旨在提供更好的链上支付网络。为实现这一目标，RSK 采用了 DECOR + 和 FastBlock5 协议，这些协议允许达到 15 秒的平均块率，而不会为挖掘集中化和自私挖掘创造激励。

主要特点：

- 块间隔 15 至 30 秒（取决于挖币者状态切换效率）
- 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。
- 新的网络命令，用于传播具有时间关键优先级的块标头。
- DECOR+ 竞争块之间的奖励共享协议。
- GHOST 链加权协议。

自从比特币创建以来，基于 PoW 区块链的加密货币的间隔越来越小。但是低块间隔可能会影响加密货币网络的稳定性和能力，因此必须考虑几个设计因素。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。影响过时块速率的主要因素是块传播协议。 对于 RSK，我们仔细分析了该协议，并且我们运行模拟以验证网络的性能、可用性和安全性。

在比特币中，当两个或更多挖币者解决了同等高度的区块时，存在明显的利益冲突。每个竞争挖币者都希望剩下的挖币者选择他的区块作为最佳链顶端，而其余的挖币者通常不会关心从这两个挖币者中选择哪一个。然而，所有剩下的诚实的挖币者和用户都有理性的偏好，即选择相同的块顶端，因为这会降低逆转概率。 DECOR +共识协议为融合选择设定了正确的经济激励，而无需挖币者之间的进一步互动。DECOR +协议是一种奖励分享策略，可以经济上进行激励解决冲突，以便：

1. 当所有各方都可以访问相同的区块链状态信息时，冲突可确定性地解决。
2. 所选择的决议最大化所有挖币者的收入（整体）和冲突中的挖币者双方，如果区块奖励差异很大
3. 如果竞争块具有大致相似的奖励，则所选择的决议最大化审查阻力。
4. 解决冲突的时间可以忽略不计。

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、ring Signatures 或 zCash 之类的匿名技术，而无需第三方信任。

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大小。使用建议的 LTCP 协议，事务大小可以减少到比特币交易规模的 1/50。这立即导致交易量能力的显著增加。此外，还有社区提案（RSKIP），以实现用户可选择的签名方案：ECDSA、Schnorr 和 Ed25519。由于 Ed25519 比比特币 ECDSA 曲线更具性能，因此使用此方案可能会带来更多容量。

RSK 功能比较

下表尝试将 RSK 的主要功能与其他备选方案的功能进行比较（包括 Liquid sidechain（Blockstream）和 WBTC 代币（BitGo））。Liquid 和 WBTC 均与 BTC 挂钩。我们表明，基本上 RSK 提出了更好的技术解决方案，对权力分散化的影响很小。

项目	比特币 BTC	以太坊 ETH	以太坊 WBTC	Liquid LBTC	RSK RBTC
平均确认时间	10 分钟	15 秒 (GHOST)	与以太坊相同	60 秒	15 秒到 30 秒 (DECOR+GHOST)
安全门槛（由于自私的挖掘或勾结）	约 30%	低于 30%	与以太坊相同	50%	50% (DECOR+GHOST)
图灵完备的智能合约	否	是	是	否	是
为比特币增加价值	-	否	是	是	是（合并挖掘）
与比特币整合	-	否	否	侧链	侧链
SPV 客户	是	是	是	是	是
Hardware 钱包集成	是	是	局部	否	是
交易终端保证	Nakamoto 一致。SHA256D	以太坊共识。Ethash	与以太坊相同	联盟	DECOR+GHOST. SHA256D PoW
保密交易	否	通过合同	否	是	通过合同原生支持计划
可扩展性[tps]	3（segwit 则为 6）	无界，现在 15	与以太坊相同	3（segwit 则为 6）	无界，现在 10
区块链大小	200 GB	> 1.5 TB	> 1.5 TB	~300 MB	~2 GB
代币挂钩安全	--	--	单一公司	联盟	联盟
代币	BTC	ETH	WBTC	LBTC	RBTC

RSK 实验室扮演的角色

RSK Labs 通过创建 RSK 节点的参考实现，使自己成为一个强大的社区参与者。RSK Labs 如今继续开展技术和社区活动，例如：

- 通过定期更新推动 RSK 参考平台的开发
- 与学术界建立合作关系
- 维护社区讨论渠道、论坛和常见问题解答
- 协调会议和本地聚会
- 推广 RSK 区块链使用
- 请求和发布定期外部安全审核
- 参与社区提议的网络升级讨论
- 安全审核 RSK 代码库
- 向政府、创业公司、企业家和公司提供有关从 RSK 网络中受益最佳方式的建议

RSK Labs 对 RSK 的持续承诺得到了 RSK 平台的奖励：20% 的平台交易费用已支付给 RSK Labs 控制的账户。

RSK 的未来

RSK 路线图由 RSK 社区建立。在 RSK 开发的最初几年，RSK Labs 在构建参考实施方面发挥了积极作用。RSK 发布后，RSK Labs 通过改进代码库并通过 RSKIP 提案存储库系统提出改进，继续高度参与社区。存储库可帮助社区成员协调多个代码库的讨论、拒绝、接受和部署。改进建议的数量巨大。以下是截至 2018 年 12 月的一些重要提案清单：

分布式内存，动态合同依赖关系，使用静态合同依赖关系的并行执行，使用运行时合同依赖关系的并行执行，转移操作，块大小限制，按代码支付的持久存储租金，无需验证的挖掘，协定的最小气体价格，交易永远不会使块无效，TXINDEX 操作码，合约休眠，支持稳定资产和代币发放，奖励经理智能合约（REMASC），简化奖励经理智能合约（REMASC），组合状态树，更简单的持久存储租金，使用 Trie 快速休眠唤醒，RS K 地址格式，生存和短暂的内存空间，高效持久存储租用，承诺 Merkle 树元素数量，Onchain PoUBS，新二进制 Trie，内存缓存，DUPN 和 SWAPN 操作码，高效存储租用，短暂 segwit，账户创建成本变更，代码分页，休眠压缩，双散列地址，CODEREPLACE 操作码，合同 const 数据部分，管理 BridgeMaster 联盟成员，交易封装，单地址智能钱包，签名压缩，多键账户，双向挂钩到比特币的基本桥接，扩展比特币桥接交易，移除世界中间状态收据，顺序地址格式，删除数据中的零字节折扣，新事件树和扩展日志，块挖掘费用信息机制，CALLNUM 操作码，通知每个块的平均可用气体，一对多集线器支付渠道，脚本版本使用 HEADER 伪操作码，内存映射配置寄存器，面向缓存的存储租用，Lumino 事务压缩（LTCP），交易金额和目的地隐私，本机概率支付，零星无验证挖掘，分层确定性钱包的衍生路径，处理比特币叉，儿童合同，校验和地址编码，面向缓存的存储租金（在 EOT 版本收取），使用状态 trie 更新批处理（COBLO）的压缩块传播，用于延迟签名聚合的双重签名，默认 TX 数据，本机离

线概率支付，更平滑的难度调整，DELEGATECALL 作为指令集扩展，管理 BridgeMaster 联盟成员

虽然有些提案尚未成熟，但其他提案经过多轮讨论后已经发展成熟，可能已获得社群支持，成为未来网络升级的一部分。

结论

RSK 是第一个生产中的比特币侧链，提供图灵完备智能合约，与以太坊标准兼容，并通过比特币合并挖掘获得保障。

RSK 代表了 5 年区块链技术改进的高潮，它使比特币生态系统能够利用可编程货币和支付的最佳功能，同时提高比特币的利用率和价值。

RSK 创新设计可实现更高的可扩展性和更低的交易成本。

RSK 使全球开发人员能够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，适合各种需求和用例。

RSK 使比特币挖币者能够参与智能合约市场，为比特币挖掘业增加重要价值并确保其长期可持续性。它有助于比特币挖币者的经济可持续性和比特币网络安全性的增长。

RSK 为以太坊用户和公司提供了一个新的兼容平台，使用比特币作为原生货币来部署他们的解决方案，依靠比特币挖掘基础设施来保障其安全性，并获得更广泛的用户群。

RSK 可以创建一个分散、安全、开放且廉价的基于区块链的金融系统，该系统将为我们这个世界上没有银行账户和经济困难的三亿多人创造包容性和机会。