

RSK推出了去中心化挂钩机制 Powpeg

直布罗陀 – 2020年12月8日

IOVlabs很高兴宣布发布Powpeg，这是对RSK智能合约平台上现有挂钩技术的重大升级。

Powpeg是一种使用工作量证明保证的双向挂钩，用于在RSK侧链和比特币区块链之间进行交互。Powpeg是第一个根据比特币的工作量证明提供安全保证的比特币挂钩，使其成为当今最安全且无需许可的挂钩。

RSK原生币RBTC与比特币（BTC）进行一对一绑定。创建RBTC的唯一方法是通过将BTC发送或“锁入”到比特币区块链中的多签名地址。该地址锁定BTC并生成该转移的证明或SPV证明，并将其发送到网桥智能合约。桥接合约获得此证明后，将等额的RBTC发送回用户。“解出”过程则正好相反。

此过程以前由一组控制多签名地址的公证人管理，解锁资金需要取得多数公证人的签名。Powpeg的发布采用了一种新的去中心化方法创建RBTC。它依靠一组负责始终保持其硬件和节点连接和正常运行的Pegnatory，但它们在交易签名中不从事任何角色。它们充当守望者，以确保将比特币存款正确通知RSK链。

Pegnatory私钥存储在称为PowHSM的专用硬件安全模块中。生成SPV证明后，它会将交易中继到PowHSM以自动执行签名过程。

Powpeg采用否决体制，任何一个实体或合谋集团均无法获得足够的权力以控制挂钩或任意审查交易。已经有十二家备受瞩目的公司参与RSK，以向Powpeg提供支持。这些参与者将在未来几周内宣布。

这标志着完全去中心化的RSK智能合约平台的重要里程碑。RSK社区正在开发其他技术，以进一步分散挂钩的权力，包括以无许可的方式推出相竞争的挂钩的能力。RSK与比特币进行合并挖掘，拥有比特币网络哈希率的50%以上。因此，这些新的创新旨在为比特币矿工提供在RSK网络中活跃的Pegnatory角色。

RSK侧链现在是一整套DeFi应用程序的大本营，例如Money on Chain和Sovryn，用户可以在其中借出、借入和交易比特币生态系统中的比特币。因此，RSK的最新努力将比特币DeFi生态系统推向了一个更加去中心化的状态，从而帮助比特币爱好者实现了无需使用集中式服务就可以进行BTC借贷和交易的目标。它还为企业家和项目参与铸造、交换BTC和RBTC开辟了新途径。



关于RSK

RSK 网络是世界上最安全的智能合约平台，并通过合并挖掘，使用比特币无与伦比的哈希算力来确保安全。

RSK通过启用智能合约、近乎即时的支付和更高的可扩展性，为比特币生态系统增加了价值和功能。

该网络可在不牺牲去中心化的的情况下扩展到每秒最多100个交易，并使用概率验证、欺诈检测等功能减少存储和带宽需求。

有关更多信息，请访问 <https://www.rsk.co/rsk-blockchain/>

