不容忽视的隐患：BTC Layer 2技术的安全挑战与威胁



本文Hash (SHA1):a9cd1d6904562d958f8347fae26c5e32cfbf63d1

编号: 链源Security Knowledge No.018



比特币（Bitcoin），简称BTC，是一个基于区块链去中心化共识，并通过点对点网络通信运行的开源加密货币系统，由全球各地的计算机网络和节点共同维护。然而，随着加密社区和生态的不断发展壮大，早期的BTC技术已无法满足用户对加密货币系统扩展性的需求。直接修改BTC底层协议不仅复杂，而且面临巨大的社区阻力，增加了系统风险，可能引发硬分叉和社区分裂。因此，BTC Layer 2 方案成为一个更为适宜的选择——通过构建新的层级在不改动BTC的前提下，兼容BTC，并满足用户对扩展性的需求。链源安全团队从L2解决方案、防护措施及未来发展等多个方面，全面分析了BTC Layer 2的安全性，希望为大家提供有价值的参考

### BTC Layer2的解决方案及潜在安全问题

BTC Layer2 是指比特币（BTC）的第二层扩展技术，这类技术旨在提高比特币的交易速度、降低手续费用，并增加可扩展性，解决BTC面临的一系列问题。目前BTC Layer2方案有很多，比较知名的有Lightning Network、Rootstock、Stacks等。另外，Liquid、Rollkit、RGB等一些项目和协议也有一定的使用场景。



1. 闪电网络（Lightning Network）

闪电网络可能是最知名的BTC Layer 2解决方案。它作为一个链下网络运行，允许参与者进行快速、低成本的交易，而无需将每笔交易记录在比特币区块链上。通过创建支付通道网络，闪电网络支持微交易，并显著减少主链上的拥堵。

使用场景：

内容创作者的微支付/点对点支付/电商和零售交易。

关键特点：

即时支付： 交易立即结算。

低费用： 费用极低，适合微交易。

可扩展性： 能够处理每秒数百万笔交易。

安全问题:

通道攻击（Channel Attacks）： 闪电网络依赖于支付通道，这些通道可能受到攻击者利用失效交易（stale transactions）或欺诈关闭（fraudulent channel closure）的攻击。

流动性问题： 如果资金集中在少数节点上，这些节点可能成为攻击目标，导致网络的去中心化程度降低。

网络分裂攻击（Network Splitting Attacks）攻击者可能尝试分裂网络，导致不同部分的网络对账单不同步。

2. Rootstock（RSK）

Rootstock，简称RSK，是一个构建在比特币上的智能合约平台。它利用比特币的安全性，同时支持与以太坊兼容的智能合约。RSK作为比特币的侧链运行，使用双向锚定机制使BTC可以在比特币网络和RSK区块链之间流动。

使用场景：

去中心化金融（DeFi）应用/在比特币网络上发行代币/跨链应用。

关键特点：

智能合约： 兼容以太坊，支持DeFi应用。

联合挖矿： 比特币矿工可以同时挖RSK，增强网络安全性。

互操作性： 将比特币与以太坊类似的功能桥接起来。

安全问题:

双花攻击（Double-Spending）： 作为侧链的RSK在某些情况下可能受到双花攻击，特别是在比特币和RSK之间转移BTC时。

智能合约漏洞： RSK允许智能合约的部署，这使得它也面临与以太坊类似的智能合约漏洞风险，如重入攻击、整数溢出等。

3. Stacks

Stacks是一个独特的Layer 2解决方案，将智能合约和去中心化应用（dApps）引入比特币。与其他Layer 2不同，Stacks引入了一种新的共识机制——转移证明（Proof of Transfer, PoX），将Stacks交易锚定到比特币区块链上。

使用场景：

lNFT平台/去中心化金融（DeFi）服务/治理和身份解决方案。

关键特点：

智能合约： Clarity，一种设计用于可预测智能合约的安全语言。

比特币锚定： 交易由比特币保障安全。

去中心化应用（dApps）： 允许开发者在比特币上构建去中心化应用。

使用场景：lNFT平台/去中心化金融（DeFi）服务/治理和身份解决方案。

安全问题:

共识攻击（Consensus Attacks）： 由于Stacks的共识机制PoX依赖于比特币网络，攻击者可能会试图通过操控比特币网络来影响Stacks的共识。

智能合约漏洞： 与其他智能合约平台类似，Stacks也面临智能合约代码中潜在的漏洞。

4. Liquid

Liquid是一个基于侧链的Layer 2解决方案，致力于提高比特币的交易速度和隐私性。由Blockstream开发，Liquid特别适合交易员和交易所，支持更快的结算和机密交易。

使用场景：

高频交易/跨境支付/代币化资产发行。

关键特点：

机密交易： 交易金额隐藏，增强隐私性。

快速结算： 交易在约2分钟内结算。

资产发行： 允许在比特币网络上创建数字资产。

安全问题:

主网依赖风险（Mainchain Dependency Risks）： Liquid作为侧链，依赖于比特币主网的安全性，任何主网的攻击或漏洞可能影响到Liquid。

私密性风险： 尽管Liquid支持机密交易，但如果密钥管理不当，隐私仍可能被泄露。

5. Rollkit

Rollkit是一个新兴项目，旨在将以太坊生态系统中流行的扩展解决方案Rollups引入比特币。Rollups将多笔交易聚合成一个批次，然后提交到比特币区块链，减少了网络负载并降低了费用。

使用场景：

可扩展的DeFi应用/微支付的聚合/高吞吐量的去中心化应用。

关键特点：

可扩展性： 显著增加交易吞吐量。

成本效率： 通过批量处理交易降低费用。

安全性： 继承比特币的安全模型。

安全问题:

数据可用性攻击（Data Availability Attacks）： 在Rollups方案中，如果数据不可用，可能导致验证者无法验证交易的有效性。

经济激励问题： Rollups需要设计强有力的经济激励机制，防止参与者试图通过不正当手段获得利益。

6. RGB

RGB是一种利用比特币的UTXO模型的智能合约系统。它旨在支持复杂的智能合约，同时保持比特币的隐私性和可扩展性。RGB专注于创建一个链下环境，智能合约可以在这里执行，并对主链的影响最小化。

使用场景：

资产代币化/隐私应用/灵活的智能合约开发。

关键特点：

基于UTXO： 保持比特币的安全性和隐私特性。

链下执行： 最小化链上的占用。

定制化： 支持广泛的智能合约应用场景。

安全问题:

智能合约的复杂性风险： RGB系统中的智能合约可能非常复杂，导致潜在的安全漏洞增加。

链下执行的可信性问题： RGB依赖于链下环境进行智能合约的执行，如果执行环境受到攻击或操纵，可能影响合约的安全性。

### 现有的安全防护措施

BTC Layer 2解决方案在提高比特币网络的可扩展性和功能性方面展现了巨大的潜力，但它也引入了一系列新的安全挑战，安全性将成为其成功和广泛应用的关键因素之一。为了应对潜在安全风险，BTC Layer2可以采取以下主要的安全防范措施：

通道安全与资金保障

多重签名和时间锁（Multisig & Timelocks）：如在闪电网络中，资金通常存储在多重签名地址中，只有在所有相关方达成共识后，资金才能被转移。时间锁机制则确保在出现争议时，资金不会永久锁定，最终可以返还给所有者。

链下交易的可靠性：通过使用链下交易，用户可以迅速进行交易，但这些交易仍需定期与主链同步，以防止双重支付或资金损失。

欺诈证明和挑战机制

欺诈证明（Fraud Proofs）：在某些 Layer 2 解决方案（如 Rollup）中，使用欺诈证明来检测和应对恶意操作。例如，如果某一方试图提交无效的状态更新，其他参与者可以通过欺诈证明进行挑战，防止无效交易上链。

挑战期（Challenge Period）：给予用户一段时间来审查和挑战可疑的交易，从而提高网络的安全性。

网络和协议的健壮性

协议升级和审计：定期审查和升级协议，以修复已知漏洞并增强安全性。例如，在 Rootstock 或 Stacks 中，代码审计和社区审查对保障智能合约的安全至关重要。

去中心化的运营节点：通过增加节点的分布式程度，减少网络单点故障的可能性，从而提高网络的抗攻击性。

隐私和数据保护

加密通信：确保所有参与者之间的通信都是加密的，防止中间人攻击或数据泄露。

零知识证明（Zero-Knowledge Proofs）：在一些 Layer 2 解决方案中，引入零知识证明来增强隐私性和安全性，避免泄露交易方的敏感信息。

用户教育和风险提示

提高用户安全意识：教育用户了解二层网络的风险，并鼓励他们使用可靠的钱包和安全的操作方式。

风险提示：在使用 Layer 2 解决方案时，向用户提示可能的风险，如链下交易的复杂性或通道关闭时的争议。

链下交易的安全性

状态通道安全（State Channel Security）：确保链下状态的完整性，并定期将状态更新提交到主链，以减少资金被盗或欺诈的风险。

这些措施共同作用，确保比特币二层网络的安全性，并为用户提供一个可靠且扩展性强的交易环境。

### 未来的安全发展趋势



行业瞬息万变，每一秒都有新的 BTC L2 诞生，但不变的是 BTC 生态向二层发展的必然趋势。BTC 就是一趟人人都想扒上去的火车，尽管面临挑战，但 BTC 生态的未来充满了无限可能。从公平分发的共识到基于铭文的扩容方案，再到追求与 BTC 共享强安全性的完全成熟的扩展方案，比特币生态正经历着历史性的变革：

解锁DeFi市场：通过启用EVM兼容的Layer 2解决方案等功能，比特币可以进入数十亿美元的DeFi市场。这不仅扩展了比特币的实用性，还解锁了以前只能通过以太坊和类似可编程区块链访问的新金融市场。

扩大使用场景：这些Layer 2平台不仅支持金融交易，还支持金融、游戏、NFT或身份系统等领域的各种应用，从而大大扩展了比特币作为简单货币的原始范围

二层网络使用零知识证明以增强安全性，Rollup技术提升可扩展性，欺诈证明确保其交易的安全性等，这些技术不仅有望显著提升 BTC 网络的可扩展性和效率，还将引入新的资产类型和交易方式，为用户和开发者开辟全新的机遇。然而，成功实现这些目标需要社区共识、技术成熟和实践验证的共同努力。在探索最有效的 L2 解决方案的过程中，安全性、去中心化和优化用户体验仍将是重中之重。展望未来，随着技术进步和社区的协作，BTC L2 技术有望释放比特币生态的新潜能，为加密货币世界带来更多创新和价值

### 结语

市场巨大的需求催生下，伴随着市场的自由竞争，一定会催生出来技术创新，L2解决方案的未来与区块链技术的整体发展密切相关，通过深入分析BTC Layer2的解决方案和潜在的安全挑战，我们揭示了其在智能合约、身份验证、数据保护等方面面临的风险。尽管当前已有多种防护措施，但随着技术的不断发展，BTC Layer2仍需在ZK技术、跨链安全、甚至量子加密等领域不断创新，以应对未来的安全挑战。随着区块链技术的进一步成熟，我们可以预见到将会出现更多的创新和变革。首先，技术的不断成熟和标准化，L2解决方案将更加稳定和可靠，其次，随着生态系统的不断扩大，比特币将在更多的场景和行业得到应用，从而进一步推动整个加密货币行业的发展。总的来说，比特币Layer 2项目的主网密集上线标志着比特币网络迈向了一个新的里程碑。