UTXO绑定：详解BTC智能合约方案RGB、RGB++和Arch Network

### 介绍

比特币是目前流动性最好且最安全的区块链。在铭文爆发后，BTC 生态吸引了大量开发者涌入，他们很快关注到了 BTC 的可编程性问题与扩容问题。通过引入不同的思路，如 ZK、DA、侧链、rollup、restaking 等方案，BTC 生态的繁荣正迎来全新高点，俨然已经成为本轮牛市的主线剧情。

然而，在这些设计中，许多都延续了 ETH 等智能合约的扩容经验，且必须依赖一个中心化的跨链桥，这是系统的薄弱点。少有方案是基于 BTC 本身的特点设计的，这与 BTC 本身的开发者体验并不友好有关。由于一些原因使得它没法像以太坊一样运行智能合约：

2017 年隔离见证 (SegWit) 的引入增加了比特币的区块大小限制；2021 年的 Taproot 升级使得批量签名验证成为可能，从而更轻松、更快速地处理交易（解锁原子交换、多重签名钱包和有条件付款）。这都使的比特币上的可编程性成为可能。

2022 年，开发者 Casey Rodarmor 提出了他的“Ordinal Theory”，概述了聪的编号方案，可以将图像等任意数据放入比特币交易中，为直接在比特币链上嵌入状态信息和元数据开辟了新的可能性，这对于需要可访问和可验证状态数据的智能合约等应用程序来说，开辟了一条新的思路。

目前，大多数扩展比特币编程性的项目依赖于比特币的二层网络（L2），这使得用户必须信任跨链桥，成为L2获取用户和流动性的一大挑战。此外，比特币目前缺乏原生的虚拟机或可编程性，无法在无需额外信任假设的情况下实现L2与L1的通信。

RGB、 RGB++和Arch Network都尝试从 BTC 原生属性出发，增强比特币的可编程性，通过不同的方法提供智能合约和复杂交易的能力：

### RGB

RGB 是 BTC 社区早期的智能合约扩展思路，其通过 UTXO 封装的方式记录状态数据，为后续 BTC 原生扩容提供了重要思路。

RGB采用链下验证方式，将代币转移的验证从比特币的共识层移到链下，由特定交易相关的客户端进行验证。这种方式减少了对全网广播的需求，增强了隐私和效率。然而，这种隐私增强方式也是一把双刃剑。通过仅让和特定交易相关的节点参与验证工作，虽然增强了隐私保护，但也导致第三方不可见，使得实际操作过程复杂且难以开发，用户体验较差。

并且，RGB引入了单次使用密封条的概念。每个UTXO只能被花费一次，相当于在创建UTXO时上锁，在花费它时解锁。智能合约的状态通过UTXO封装并通过密封条管理，从而提供了一种有效的状态管理机制。

### RGB++

RGB++ 是 Nervos 在 RGB 的思路下的另一条扩展路线，依然基于 UTXO 绑定。

RGB++ 利用图灵完备的 UTXO 链（例如 CKB或其他链）来处理链下数据和智能合约，进一步提升了比特币的可编程性，并通过同构绑定BTC来保证安全性。

RGB++采用图灵完备的UTXO链。通过使用像CKB这样的图灵完备UTXO链作为影子链，RGB++能够处理链下数据和智能合约。这种链不仅可以执行复杂的智能合约，还可以与比特币的UTXO进行绑定，从而增加了系统的编程性和灵活性。此外，比特币的UTXO和影子链的UTXO同构绑定，确保了状态和资产在两条链之间的一致性，从而保证了交易的安全性。

除此之外，RGB++不仅扩展到所有图灵完备的UTXO链，不再局限于CKB，从而提升了跨链互操作性和资产流动性。这种多链支持允许RGB++与任何图灵完备的UTXO链结合，增强了系统的灵活性。同时，RGB++通过UTXO同构绑定实现无桥跨链，与传统的跨链桥不同，这种方式避免了“假币”问题，确保了资产的真实性和一致性。

通过影子链进行链上验证，RGB++简化了客户端验证过程。用户只需检查影子链上的相关交易，即可验证RGB++的状态计算是否正确。这种链上验证方式不仅简化了验证过程，还优化了用户体验。由于使用图灵完备的影子链，RGB++避免了RGB复杂的UTXO管理，提供了更加简化和用户友好的体验。

### Arch Network

Arch Network 主要由 Arch zkVM 和 Arch 验证节点网络组成，利用零知识证明 (zk-proofs) 和去中心化验证网络确保智能合约的安全和隐私，比 RGB 更加易用，并没有像 RGB++ 一样需要另一条 UTXO 链进行绑定。

Arch zkVM使用RISC Zero ZKVM执行智能合约并生成零知识证明，由去中心化的验证节点网络进行验证。该系统基于UTXO模型运行，将智能合约状态封装在State UTXOs中，以提高安全性和效率。

Asset UTXOs则用于代表比特币或其他代币，并可通过委托的方式进行管理。Arch 验证网络通过随机选出的leader节点对ZKVM内容进行验证，并使用FROST签名方案聚合节点签名，最终将交易广播到比特币网络。

Arch zkVM 为比特币提供了一个图灵完备的虚拟机，能够执行复杂的智能合约。每次智能合约执行后，Arch zkVM 会生成零知识证明，这些证明用于验证合约的正确性和状态变化。

Arch 也使用了比特币的 UTXO 模型，状态和资产被封装在 UTXO 中，通过单次使用的概念进行状态转换。智能合约的状态数据被记录为 state UTXOs，而原数据资产被记录为 Asset UTXOs。Arch 确保每个 UTXO 只能被花费一次，从而提供安全的状态管理。

Arch 虽然没有创新区块链结构，但也需要一个验证节点网络。在每个 Arch Epoch 期间，系统会根据权益随机选择一个Leader节点，Leader节点负责将收到的信息传播到网络内的所有其他验证者节点。所有 zk-proofs 都由去中心化的验证节点网络进行验证，确保系统的安全性和抗审查性，并生成签名给Leader节点。一旦交易由所需数量的节点签署，就可以在比特币网络上对广播。

### 结论

在BTC可编程性设计方面，RGB、RGB++ 和 Arch Network各有特色，但都延续了绑定 UTXO 的思路，UTXO 的仅一次使用的鉴权属性更适合智能合约用于记录状态。

但其劣势也非常明显，即糟糕的用户体验，与 BTC 一致的确认延迟与低性能，即只扩展了功能，但没有提升性能，这在 Arch 与 RGB 中较为明显；而 RGB++ 的设计虽然通过引入更高性能的 UTXO 链提供了更好的用户体验，但也提出了额外的安全性假设。

随着跟多开发者加入 BTC 社区，我们会见到更多的扩容方案，如 op-cat 的升级提案也在积极讨论中。而切合 BTC 原生属性的方案是需要重点关注的，UTXO 绑定方法是不升级 BTC 网络的前提下，扩展 BTC 编程方式的最有效方法，只要能解决好用户体验问题，将是 BTC 智能合约的巨大进步。