聊聊OP\_Codes：AVM将如何“重启”比特币编程时代

作者：Leaper

比特币作为“数字黄金”，多年来只被视为价值存储的标的。

有没有人想过，这是一种迫不得已的行为？

有没有可能，曾经的比特币其实是有办法、有机会拥有以太坊那样的繁荣生态与复杂应用，但是“不得不”被拦住了脚步。

这是中本聪退隐之前的一大决策——为了安全（避免潜在的拒绝服务攻击），而禁用了一系列的原始操作码（OP Codes），这些操作码本用于二进制操作与复杂计算，本可以实现高级脚本的编写。

其中比较知名的是OP\_CAT，数据连接操作码，如今，人们也在谈论重启它的计划（BIP-420）。

那时候的比特币，还不敢如此激进。于是相对保守的措施限制了比特币上的智能合约发展。

于是，一直以来都有人在思考：如果当时比特币没有禁用原始操作码，比特币生态会如何发展？比特币又可能遇到什么样的安全问题？

其实，已经有几场巨大的社会实验在探索这个问题，如BSV、BCH。在这些比特币的分叉版本中，原始操作码不仅仅高度拓展了生态开发潜力，并且在多年的实验证明下告诉币圈——他们不会引发任何安全问题或拒绝服务攻击。

那么，OP\_Codes 有可能得到重启吗？什么时候重启最为合适？今天，逐步繁荣的比特币生态给出了答案。

随着比特币自身的发展，今天，“可拓展性”正在重回比特币。Ordinals、Atomicals、Runes、Stamp……诞生了无数的拓展协议与标准，在如今的比特币主网风起云涌。

越来越多可能性能够在如今的比特币基础环境下得到技术实现，其中，也包括了Atomicals协议下的AVM（Atomicals Virtual Machine, 原子虚拟机）概念，旨在通过模拟比特币虚拟机在比特币上实现智能合约。

Atomicals协议创始人Arthur认为，我们可以通过某种方式，全面开放OP\_Codes，彻底解放比特币原生编程能力。

这一切可能性一开始就存在，只是那时候它不适合走向世界。今天的比特币已不同往日，“比特币生态”的发展空间被全面打开。

AVM的实现，本质上是在协议虚拟层提供了测试原始操作码的平台，所有人都可以基于AVM方法来测试与应用比特币的原始操作码。也有人将它比喻为“云比特币”。

在现在的比特币生态里，我们看到的铭文、符文、邮票等数字资产类别，可以被视为一种基于比特币的“叠加协议”，而AVM，不对比特币本身进行修改，而是在这一层面针对叠加协议创造了一种方法，所有叠加协议（不限于Atomicals）都可以主动采用AVM。这一解决方案其实是比特币生态及此类叠加协议自然演化发展的结果，为整个比特币生态提供了原始操作码的开发平台。

“我们提出了一种通过模拟比特币虚拟机及其脚本解释器来为各类叠加数字资产创建和执行智能合约的方法。在这种方法中，比特币区块链不仅为链上存储的智能合约程序提供时间戳和数据，同时，这些程序的执行也通过各种叠加协议索引器在一个沙盒环境中进行。叠加协议索引器节点由应用程序开发者、服务提供者和用户共同管理，共同形成了一种自发的共识。这一概念及其技术可广泛适用于所有叠加协议，只需要针对各自的叠加协议索引器作适当调整即可。”

——AVM白皮书段落节选

在比特币资源有限的环境下，原生的OP\_Codes是最高效的编程方式。它本就属于比特币，在足够安全的环境下，它是比特币的技术拓展最优解。

如果说，当年的比特币被禁用OP\_Codes后不得不只作为“数字黄金”，那么这一次AVM将OP\_Codes带回比特币就是一次巨大的比特币应用实验，这一次，我们将见证比特币能否“不仅仅是数字黄金”。打开了想象空间的比特币会如何发展？从数字黄金到黄金生态、黄金产业链、复杂的黄金金融体系……把AVM后的比特币生态称之为 “Bitcoin 2.0” 并不为过。

其实，很多比特币开发者也认为，比特币自身的操作码重启很可能是历史的大势所趋。而AVM，提前走向了可能出现的未来。白皮书坦言：“我们希望比特币最终能够重新启用所有原始操作码，从而释放中本聪创造的最大潜力。”

比特币能不能有生态？比特币该不该有生态？AVM会给我们答案。