# BTC生态以太坊ETH程序软件开发

| | |
|---|---|
| 产品名称 | BTC生态以太坊ETH程序软件开发 |
| 公司名称 | 河南漫云科技有限公司 |
| 价格 | 1000.00/件 |
| 规格参数 | 漫云科技:BTC生态以太坊ETH程序软件开发 |
| 公司地址 | 郑东新区升龙广场3号楼A座3202 |
| 联系电话 | 13103827627 13103827627 |

# 产品详情

比特币生态不是建立在Layer1之上的，比特币qukuailian天然不是图灵完备的，而且，比特币极简的UTXO和有限的区块空间也无法处理复杂的数据和计算。因此，比特币要发展生态必需Layer2，而且是完全去中心化的比特币Layer2。比特币15年来的几次重大升级带来了许多技术革新，但是，一直被人们忽视，因此，大部分人认为，比特币生态做不出完全去中心化的可以支持大规模生态应用的Layer2。这是对比特币的发展缺乏认知，对Layer2的本质缺乏理解，对比特币生态带有傲慢和偏见。

阻碍人们进步的大障碍，正是傲慢与偏见。我劝诸君，放下傲慢，空杯学习，端正认知。谨以此文，为去中心化的比特币Layer2正名。

正文：

一、什么是Layer2？Layer2的本质是什么？

二、比特币Layer2和以太坊Layer2在设计上会有哪些异同？Layer2的设计原则是什么？

三、比特币Layer2的正确道路

四、比特币Layer2必将超越以太坊Layer2，比特币生态必将超越以太坊生态

一、什么是Layer2？Layer2的本质是什么？

Layer2的概念被人们熟知是因为以太坊生态，但是，Layer2的概念却不是以太坊生态原创，而是来源于比特币。

比特币0.1版本的代码里保留了一份原始版本的代码，是中本聪留下的。这段代码支持用户在交易被矿工打包确认之前更新交易。如果一个用户的余额增加，另一个用户的余额就会相应减少，一旦用户完成了交易，他们就可以只向主链网络传输一个交易结果然后关闭他们的支付通道。基于“ 支付通道“ 后来诞生了闪电网络，闪电网络是比特币早的Layer2，也是加密世界里早且可行的Layer2。

因此，在我们谈什么是Layer2时，不能仅以以太坊Layer2马首是瞻，也不能以以太坊Layer2为唯一衡量标准（毕竟以太坊Layer2是经过这两年的发展才基本确定了roullp这个设计方向的可行性），而是应该透过现象看到本质，需要了解Layer2的本质是什么？这样才能设计出切实可行的Layer2。

无论是比特币Layer2还是以太坊Layer2，其诞生的背景都是当Layer1主网无法实现更复杂更高性能的应用场景时，需要把Layer1资产跳脱到Layer2去实现。以太坊需要Layer2去拓展其性能，比特币则更需要Layer2。比如，BTC可以在闪电网络里实现快速高效的支付场景；ETH则可以跨到Arbitrum去速度更快、Gas更低且更复杂的智能合约场景。

因此，无论是比特币Layer2还是以太坊Layer2，其本质都是一样的，都是让Layer1的主网资产跨到Layer2实现更复杂更高性能的应用场景。因此，Layer2的本质是一个去中心化的跨链方案+一个高性能且无需信任的二层网络。

那么，无论是比特币Layer2还是以太坊Layer2，在设计时都得遵循一些基本的原则：

1、必须实现Layer1资产无需信任地跨到Layer2，这是重要的步。

2、Layer2网络的账本一定是安全且无需信任的。

只有同时满足以上两个条件，才是一个切实可用且完全去中心化的Layer2。

二、比特币Layer2和以太坊Layer2在设计上会有哪些异同？

我们搞清楚了Layer2的本质是什么，也搞明白了Layer2设计的基本原则，那么，我们来看一下，比特币Layer2和以太坊Layer2在实际设计上有哪些异同？

1、必须实现Layer1资产无需信任地跨到Layer2

以太坊Layer1和Layer2之间的跨链方式：Layer2官方在以太坊主网首先部署一个托管资产的智能合约，当用户从以太坊主网把ETH跨到Layer2，用户的ETH被锁定在该智能合约并在Layer2网络1:1生成新的ETH。当用户发出跨回主网的指令时，Layer2的ETH销毁，同时触发Layer1上的智能合约把ETH解锁给用户。这是以太坊Layer1和Layer2的跨链实现方式。是通过以太坊的智能合约以及Layer1和Layer2网络通讯实现的，可以实现去信任化。

那么，比特币的Layer2该如何实现去信任的BTC跨链呢？

在2021年比特币Taproot升级之前，是无法做到完全去中心化的BTC跨链的，但是，由于Taproot升级带来了Schnorr签名和MAST合约，让完全去中心化的比特币跨链成为现实。

Schnorr签名是一种比椭圆曲线签名更适合比特币的签名算法，以太坊也一直想支持该签名，但是由于升级签名算法涉及以太坊的账号体系等复杂问题，因此以太坊一直没有升级为Schnorr签名。Schnorr签名大特点是聚合签名，可以实现1000个比特币地址来签名管理同一笔资产，不仅可以实现签名的隐私性，还可以让1000个签名提交的数据并为一笔，彻底解决多重签名带来的数据堆积问题，因此，Schnorr签名可以突破原来比特币多15重多签的限制，实现完全去中心化的签名管理。

而Mast合约，全称MerkleAbstractSyntaxTree，是使用默克尔树来加密复杂的锁定脚本，其叶子是一系列相互不重叠的脚本，支出时，只需披露相关脚本以及从该脚本通向默克树根的路径。

简单理解Mast合约就是等效于VM的功能（类智能合约功能），可以通过指令来执行既定的操作，比如，Mast合约+Schnorr签名的组合，可以通过触发Mast合约来让参与去中心化资产管理的1000个节点进

行签名，从而智能化地按照合约制定的规则来执行比特币的进出与花费，这里没有任何人为的干预，完全靠合约执行，从而实现比特币的去中心化管理。具体细节可以参考BEVM白皮书：https://github.com/btclayer2/BEVM-white-paper

我们以BTCLayer2项目BEVM为例，来看，真正的BTCLayer2是如何实现完全去中心化跨链的？

当用户把比特币主网的BTC跨到BEVM时，用户的BTC进入1000个节点托管的合约地址内，然后，同时在BEVM即BTCLayer2网络按照1:1的生成新的BTC，当用户发出把BTC从BEVM跨回主网的指令时，BEVM网络节点将触发Mast合约，1000个托管资产的节点将按照既定的规则自动签名，把BTC返回到用户地址。整个过程，实现了完全的去中心化和无需信任。

从以上内容可以看出，通过使用Taproot带来的Mast合约+Schnorr签名的组合，比特币也可以和以太坊Layer2一样实现完全去信任的跨链，这是实现完全去中心化的BTCLayer2重要的步。

2、Layer2网络的账本一定是安全且无需信任的。

以太坊Layer2的账本是由排序器管理，在处理交易时，是按照一定比例，一般是10:1的比例，把Layer2的账本roullp后打包上传到以太坊主网，然后由以太坊节点验证，但是，以太坊Layer2的排序器（就是Layer2网络的运行节点，一般都只有1个节点）是完全中心化的，均是由Layer2官方来运行和掌握，如此中心化的设计如何取得用户信任呢？主要是通过把Layer2的账本roullp打包到以太坊主网让矿工节点验证，如果用户不信任该账本，可以通过发起链下检举来验证账本，因此，Op-Roullp又被称为乐观证明，就是其信任假设是乐观地认为官方不作恶，如果作恶，可以通过检举来证明。这些组合设计，基本可以保障Layer2账本是可信的，但是，这也导致以太坊Layer2上的ETH等资产是不抗审查的，是可以被外部力量强制冻结的，因为，ETHLayer2排序器就官方自己一个节点，是可以被中心化控制的。这也将导致ETHLayer2的资产规模是有上限的，因为，很多大资金将因为不抗审查的问题而不敢进入，试想，如果你有10万枚ETH，你敢把这些资产跨到一个不抗审查的以太坊Layer2吗？

同时，这里还衍生出两个对于用户不友好的问题：

a、由于Op-Roullp有一个7天期限的检举机制，因此，当用户把ETH从Layer2跨回以太坊主网时，至少需要过完7天的检举期。

b、由于ETHLayer2的排序器完全是项目官方一个节点在控制，因此，ETHLayer2的跨链及交易手续费完全由项目官方独享的（据悉Base、ZKsync等ETHLayer2每月排序器营收超500万美金，高峰时超1000万美金），而Layer2用户无法分享这些网络增长红利。