对话RGB++提出者Cipher：我眼中的RGB++和UTXO以及BTCFi



2024年7月22日，极客Web3有幸邀请到CKB的联创及RGB++提出者Cipher，就其眼中的RGB++与UTXO体系、CKB本身和比特币生态进行了一系列交流，期间Cipher谈到了自己的过往经历、RGB++ Layer与UTXO模型对BTCFi的独特意义、关于CKB和比特币生态的一些问题与看法。本次访谈涉及的具体问题包括：

1. Cipher个人经历

2. UTXO Stack和RGB++ Layer的联系

3. 对比特币二层和BTCFi的看法，尤其是EVM系二层

4. RGB++ Layer相比于EVM系的独特场景与发展理念

5. 对CKB本身设计理念的解读

6. 如何解决UTXO模型在Defi生态建设上的一些不足

7. CKB为何选用RISC-V以及相关的合约开发语言选择

8. 对比特币和以太坊生态在去中心化问题上的看法

以下为本次访谈的文字版记录，欢迎大家仔细阅读。

Faust：首先请Cipher来自我介绍一下？

Cipher：我最早接触区块链是在2013年，因为参与比特币挖矿而入圈，那时候挖矿还没那么卷，结果我第一次买矿机就遇到了黑心厂家。到了14～15年时，因为比特币价格波动很大，我写了个自动炒币的程序，赚了一点钱。15年底熊市来了，我暂时离开了币圈，当时我还没有建立起信仰，只是投机。

到了2016年，我正式进入了区块链行业，进了体制内的区块链研究院，参与了央行的数字货币及联盟链的开发，职位是产品负责人。期间我还写了一些白皮书，以及行业早期的隐私保护文件，以及数字产权相关的专利。

18年的时候，我彻底意识到联盟链是错误的方向：所有的联盟都会有盟主，有盟主就没必要去用区块链，如果是国字头下面的联盟链就更没意义了，只是盟主的一言堂。后面我的工作重心转向无需准入许可的公链。机缘巧合下，我和几个伙伴参与了CKB的早期建设，我当时负责产品和一部分研究工作。

大概到了2021年，我逐渐从CKB基金会独立出来，成立了自己的公司，做CKB生态内的周边项目，比如JoyID这种。目前JoyID有了超过50万的用户，可以说是业内最完善的Passkey钱包，虽然Passkey本身在设备兼容性上存在一些限制，但我们的钱包还是很好用，可以直接免手机号邮箱和助记词，在安全模型上是非托管型钱包。

到了2023年的铭文之夏，整个比特币生态开始回暖，甚至文艺复兴。今年2月中旬，我提出了一个概念，即RGB++，愿景是给BTCFi创造原生的智能合约环境，同时不丧失比特币的安全性。对此我们迅速成立了专向小组，赶在今年4月比特币减半前上线了RGB++协议，效果还不错。同时CKB生态内的一些项目，包括DEX、Launch pad、算稳也都陆续上线了。整体上看，RGB++生态正处于蓬勃向上的阶段。

在解决了对BTC的功能拓展问题后，我们又把目光聚焦在了扩容等方面。4月份我们专门成立了一家公司，去做启动UTXO公链或比特币二层的UTXO Stack。至于为什么选择UTXO模型，最核心的是比特币本身就是UTXO模型，而且和以太坊差异甚大，如果在比特币上做Layer2，状态转换证明、跨链、资产强制退出和DA等部分该怎么实现？如果照搬以太坊的账户模型和Rollup那套思路，很难得到好结果。这也是我一直以来的观点：照搬以太坊的思路到比特币上，很难有善终。

UTXO Stack目前完成了第一轮融资，第二轮融资也在进行，虽然近期比特币生态的热度有所下滑，但我们还是很有信心，愿意把大旗扛起来，为BTCFi搭建近乎原生的功能拓展与可编程生态。目前我们做了更多关于市场和商务层面的工作，一些生态相关的活动也会接踵而至，大家可以期待这方面的进展。

雾月：UTXO Stack和RGB++Layer是什么关系？两者好像有从属的关系？这方面可以好好介绍下？

Cipher：二者的关系可以分两个角度来介绍。从品牌角度看，RGB++Layer是隶属在UTXO Stack大品牌下的产品；从技术角度看，RGB++Layer利用同构绑定给BTCFi增加了智能合约执行层。同构绑定不但适用于BTC和CKB，还适用于Cardano、Fuel和Sui等广阔的公链生态，只要和UTXO沾边即可。

至于UTXO Stack有点类似于OP Stack，可以用于快速启动BTC Layer2，它直接附带同构绑定功能，可以将主网的BTCFi资产通过Leap的方式转移到Layer2上去做交易。OP Stack的智能合约跑在以太坊上，UTXO Stack的智能合约跑在RGB++ Layer上。

回到两者最终的从属关系和优先级，这涉及到一个逻辑问题：所有L2成立的前提，基本都是L1已经足够拥堵，或者是L1功能有限不能满足用户需求。

目前来说，比特币+ RGB++layer构成的这样一个智能合约层上，还没涌现出那么多资产和应用，所以我们希望把新的开发者和用户先引导到RGB++Layer上，去做Defi应用、交易平台和资产发行，把BTCFi生态先发展起来再深入去做L2的工作。只有等到BTCFi本身有足够的热度，BTC扩容才能成为真正的需求，这时UTXO Stack的推出就水到渠成了。

Faust：这里您提到BTC二层的事，近期我们从一些渠道得到的消息也是认为，BTC Layer2到了阶段性谷底，更多人或机构把注意力放到了BTCFi这块。但很多BTCFi只是WBTC的模式，把比特币桥接到其他公链或者比特币侧链上去，根本就不BTC Native。在您看来，BTCFi和WBTC这种东西的真正区别在哪里？

Cipher：我一贯的观点是，EVM系的BTC Layer2天花板很低，理由很简单，用EVM的话就不是在为比特币壮大其生态，而是把BTC引入到其他生态。我们知道，比特币主网上很难实现智能合约，TPS也高不了，那有个很简单的办法：把比特币桥接到别的地方。这样看着可以解决问题，实际却避开了最核心的东西：

在这种方式下，比特币自己的生态根本就没有得到发展，比特币矿工收入、链上数据之类的不会有任何变化，你做的只是最简单的资产桥出，桥出之后你就能得到新故事新场景吗？显然不能。因为你做的所有事情，是WBTC和以太坊生态很早就做了的，没有任何创新，只不过多创建了一种BTC桥接资产。那么你存在的意义在哪里？

同样是EVM，难道你还能超越以太坊上已经存在的DeFi体系吗？EVM系的比特币二层短期内可能因为空投预期而创造出虚假的繁荣，但长期发展很容易受限。能够长期影响并赋能比特币生态的，一定是更原生、基于UTXO的Layer2。

而所谓原生BTC二层，其吸引人的点不在于什么正统性，而是这种“原生”可以为比特币生态带来更有趣的场景。比如说，RGB++有一种技术叫无桥跨链Leap，BTCFi资产可以在L1到L2或L2之间来回跳转，这种方式可以不需要依赖于传统跨链桥的Lock-Mint范式，可以规避传统跨链桥的很多风险，在跨链响应速度以及流动性聚合上也有很大优势，可以为Defi生态带来很大便利。Leap功能从4月就开始上线了，很多用户都在享受着该技术带来的便捷。这个就是比特币原生方案带来的创新之一。

此外还有一点，是否有BTC原生属性也会影响受众。比如，很多BTC持有者连Metamask都不怎么喜欢用，更喜欢用BTC生态里已有的主流钱包。虽然有一些所谓的AA方案，可以让比特币钱包在EVM应用层去做账户抽象，但这种方式存在各种问题，会阻碍BTC持有者的进入。而像我们这种基于UTXO的二层方案，直接支持用比特币钱包来交互，它的AA实现方式更贴近底层，用户可能都感知不出来，这非常便捷，更简单，更易用，更无缝。

此外我们知道，UTXO模型是“链下计算，链上验证”，这种模式特别适合intent驱动的交易场景。所谓intent就是，我这笔交易只告诉系统，我愿意付出什么，需要得到什么，但中间怎么调用智能合约、怎么设置函数参数等，我根本就不用操心，我把我想要的input和output结果放链上去验证了即可。如果要在以太坊上做Intent场景，可能需要Operator、Aggregator等一系列组件，比较臃肿，但在UTXO世界就很简单。这也是UTXO二层相较于EVM二层的特色。总之，我们比较看好UTXO能为Layer2催生出的新DeFi场景。

Faust：RGB++Layer和BTC的主要结合点都有什么，哪些场景最重要？接下来RGB++和CKB最核心的生态布局以及路线图包括什么？

Cipher：二者的结合主要还是在于各种应用场景。有一些场景刚才已经讲到了，下面再举一些例子。我们知道以太坊生态里闪电贷很有存在感 ，它可以在一笔交易内连续调用一系列合约，得到交易结果并向借贷平台展示：我向你借出的资产和利息都能在瞬间返还给你。我们可以利用链上闪电贷快速进行各种金融活动，但在UTXO世界里是没有闪电贷的，但却有其他东西。

比如，UTXO有合约脚本嵌套的机制，可以连续生成一系列交易，简化用户的交户流程，上一笔交易的输出结果，可以直接作为下一笔交易的输入参数，通过这种方式我们可以快速生成一批首尾彼此衔接的交易指令。那我举个例子，比如现在要做一个跨链DeFi，先把资产从A链跨到B链，再去DEX里卖掉一半，之后与没卖的那部分Token组成一个LP对，放到流动性池里。这四步操作在RGB++Layer的智能合约框架里，可以用上面说的合约脚本嵌套方式来一键式的实现。这意味着上述一整套流程，用户只需要操作一次，剩下可以由去中心化智能合约自动操作完成。

还有一个明确的结合点，就是IB0，即通过比特币来融资。当然这也不是一件新鲜事了，以太坊就是走的这种融资方式，早期是一个比特币可以换一万还是两万以太坊。但是过去IB0的问题就在于，虽然跟IC0同样是融资，但资产融完却并没有什么玩法。我举个例子，像一些IC0，它有一个明确的价格曲线，比如前100-200个区块往后，购买价格呈现阶梯式的上升或下降，还有的是最开始买的人需要锁一个月，最后一个买的人可能需要锁三个月。再比如多锁一个月多给50%的币，锁一年多给100%，类似这样有很多不同的方法。

此前，这类特殊规则在IB0身上无法实现，而我们可以通过RGB++ Layer来改变这点。比特币资产一大问题就是没有可编程性，相当于只能发行Meme币，而一旦可以和智能合约结合，就意味着可以给资产赋能。这些东西打通了后才有项目方愿意来比特币生态建设。

对于BTCFi或任何Fi而言，前提是要有资产和对应的丰富场景，如果这个资产只局限于BTC本身的话，往往只能搞远程质押、跨链等单一场景，若真想让生态繁荣起来，需要发行各种资产来百花齐放。现在的以太坊世界，ERC-20资产和ETH本身市值应该是差不多的，甚至后者比前者还多，而比特币生态的非BTC资产可能连BTC市值的1%都不到。所以怎么在BTC生态把新的资产创造出来，是发展关键。

所以我觉得RGB++ Layer和比特币最大的结合点是，利用RGB++Layer的可编程能力，创造真正赋能比特币的去中心化资产类别，以前这件事在比特币身上从没有出现过，要么就是Memecoin要么就是中心化资产。总之，我们非常看好利用智能合约层为比特币生态创造新资产的可能性。

Faust：CKB在18~19年的时候，自我定位是“专为Layer2设计的Layer1”，在为Layer2做状态结算等场景上做了很多配套的设计，可以说是为Rollup专门设计的去中心化验证层。对此，您认为CKB相比于普通公链，其核心优势是什么？

Cipher：其实很难定义比特币生态里什么叫一层什么叫二层。我觉得CKB和RGB++Layer并不是立足于为某个二层去做验证和结算。CKB作为一个UXTO链，擅长的点本就偏向于验证链下的计算结果，而不是直接跑链上去计算，这是CKB最初创立的时候，Jan作为首席架构师非常坚持的一个点，他认为区块链的计算资源、存储资源、带宽资源都极其珍贵，不应该用它来做任何复杂的工作，而应该做最简洁的事情。

实际上，无论是对Layer2还是Layer1，都要就状态变更一事做共识，而做共识只有两种办法，一是把执行状态变更的合约拿过来，每个人都算一遍，得到同一个结果以达成一致，这就是账户模型的逻辑；二是你在链下完成状态变更，你把证明其有效的Proof发给我，我验算这个Proof就行，不用自己亲自算一遍原始的内容，这其实就是现在Rollup的思路。

第二种办法我们在2018年提出来的时候，大家还觉得怪怪的，计算一遍和验证一遍似乎是同一件事情，但Jan说其实是不一样的。比如排序算法，验证结果的复杂度远小于直接计算的复杂度。当时很多人觉得，普通的ERC-20资产转移根本没必要这么做，但后来的故事大家都知道了，不论是ZK也好，还是Rollup也罢，都是链下计算链上验证的范式。这个时候你才会发现，第二种方法是更有效且有价值的。

UTXO模型对于并行计算也有很多好处。我们知道以太坊最近在提并行EVM的叙事，但通过一些渠道我了解到，所谓的并行EVM，其投入实际使用后并行度很多时候连2都达不到。而UTXO天生就支持并行计算，有多少个CPU核心，就能并行多少个线程，这种效率不是基于EVM的东西能比的。

我们从5年前就在走UTXO这条路，在我们刚才描述的若干场景里，UTXO天然就比账户模型有更多优势。而且我们和比特币都是UTXO，可以支持同构绑定，使一些功能得到进一步简化。所以我觉得，主要优势还是架构上，采用UTXO这种架构去对接比特币，我们肯定更高效。

Faust：有人认为UTXO不利于支持DeFi，比如不同的UTXO之间状态没有办法互相调用，甚至于认为RGB++和CKB如果直接在一层上发展Defi生态会遇到阻力。对于这些观点你怎么看？以及你们推出了什么方案解决这些问题？

Cipher：首先这些看法存在一定的合理性，因为账户模型符合更直觉，和以前单机程序一样，考虑一些攻击场景就ok了。而UTXO模型不是，你在链上写的合约是验证器，还要在链下构建一个专门的计算器，我们通常称之为Aggregator聚合者，或Gennerator生成者。Gennerator负责在链下计算状态将其生成，再丢到链上去验证，这相对比较复杂。

如果是像UTXOSwap这种基于UTXO的DEX平台，你很难在发起交易时就知道结果，因为可能同时有100个人去提交操作，但UTXO的特殊属性，会要求100个人里，同一时间只能有1个人改写其状态，这时候就会出现争用问题。如果不对这些彼此有冲突关系的交易请求做处理的话，最终可能100笔交易只有1笔成功，剩下99笔交易全部失败。这个问题对产品设计是一个极大的挑战，这也是为什么大家说UTXO模型不利于DeFi。

但我们同时也看到，即使在近两年，也有新的UTXO链涌现出来，比如Fuel。为什么明明有各种麻烦，还有人去前赴后继地用UTXO模型呢？因为它有很多优势，之前我也都有提到。那回过头来，这些问题怎么克服？我们经过5年的打磨，已经有了非常成熟的解决方案，可以在UTXO链上实现类似Uniswap的功能。生态里的UTXOSwap也是不久前上线主网的，已经有很多人在加LP和交易对了。如果你真去体验的话，会发现它跟Uniswap几乎没有任何区别。

其实UTXOSwap的设计也很简单，我们把每一笔交易分成了两步，第一步是用户把他的意图提交上链，第二步由Aggregator去聚合所有人的意图，合并后发起一笔交易和流动性池做交互。流动性池可以一次性满足这些意图，针对结果生成一个最终的UTXO。

这里可能有一个区块延迟的问题，因为第一步中，用户要先把自己单独的意图发上链，由聚合者/排序器打包处理后，在由后者链上进行下一步操作。不过在实际操作中，用户可以直接在链下把交易意图发给Aggregator，由后者批量处理，这样就能解决响应延迟的问题，实际上和Rollup差不多。UTXO的这些问题，我们已经有很成熟的解决方案了，CKB这边也在做一些方案去实现上面提到的这类流程。

还有一个方面，UTXO很适合支持订单簿模型。在以太坊上过去是有订单簿模式DEX的，但后来销声匿迹了，这里面原因很多，最核心的原因是订单簿DEX不适合在账户模型上运行，因为每笔挂单和撤单哪怕没成交都要付手续费，这个对PMF来说是不可承受的，所以后来出现了AMM模型。但在UTXO模型下就会有所不同，比如可以同时挂100个单，在UTXO世界里一笔交易关联到100个UTXO是很容易且低成本的事，你想的话还可以挂更多。所以UTXO模型下，订单簿DEX会更有用武之地。

更何况我们还有PSBT部分签名技术，挂单交易甚至不需要提交上链，你发一个简洁的签名就行，由撮合者把多方签名聚合后一起把交易上链，这样一来订单簿模式就更适配UTXO模型了。包括AMM也是，可以像UniswapV3一样采用区间阶梯价格，来提供虚拟流动性，在不同的价格上放不同的流动性份额，而不是一条平滑曲线。

这些都是UTXO环境下独特的DeFi场景，都是相当高级别的创新。而这种级别的创新，不太可能在一条EVM链上去做，EVM链上更多的是Copy类山寨项目，根本没有创新想法。我们想真正吸引比特币生态的原生开发者，或者是热爱UTXO模型的开发者，这些开发者往往有很强的能力和创新驱动力，我们也非常看好在这种模式下可以有新的BTCFi范式出来。

Faust：CKB用的是RISC-V指令集，能支持多种编程语言。然而有人认为，支持的编程语言太多也不是好事，会让一条公链的开发者生态变得混乱割裂。对此，您认为目前在CKB上做开发首选的语言是什么？

Cipher：目前来说，首选还是Rust，其次是C，这两个都有比较完善的支持。RISC-V目前已经是一个主流的CPU架构了，可以预见5到10年内即可超越ARM，它支持的编译器也非常多。但目前CKB官方支持更多的还是Rust和C，同时也支持一些脚本语言。我们自己也做了一些Runtime，来支持LUA和javascript这种，但性能折损会很大，极限的话可能是30%到300%的降速。所以如果是算法密集型的业务，还是推荐用Rust或者C去写，并且也不会有太多的编程语言去割裂开发者生态。

我其实想讲讲RISC-V本身的优势，18年刚做CKB时，我们是全球唯一一个选择用RISC-V做公链虚拟机的，原因很简单，RISC-V是适用于硬件设备的指令集，它的设计有两个特点：精简和谨慎。既然是针对硬件做的指令集，往往比较稳定，不会像EVM那样每年增减指令，这种谨慎正是开源协议需要的。

其次，对于智能合约平台或者区块链来讲，我们认为最好就像比特币一样，其核心功能趋于固定，不然三天两头增减内容太容易出问题，可以说我们整个的思路就和以太坊不一样。EVM基本每年都有对操作码的迭代，过去几年都是如此，这对于程序的兼容性、稳定性都会产生影响，对此我们极力避免。所以我们基于这种思路，采用了RISC-V指令集，事实证明这非常有前瞻性。

而今ZK开始大行其道，你会发现很多项目方在底层用RISC-V做虚拟机，那我们作为基于RISC-V的公链，再去兼容新的ZK设施就非常容易，从指令层面就不需要任何翻译，效率显然比在EVM上跑RISC-V高太多。

Faust：站在CKB的视角，你们对比特币生态怎么看？比如你们认为现在比特币生态里，有没有出现类似于以太坊基金会那样的中心化组织？之前有人认为BlockStream就有点独断专行，CKB对此是否有自己的看法？

Cipher：我觉得比特币生态和以太坊生态相比，结构完全不一样。以太坊基金会有非常强的话语权，反观比特币世界，你可以说它背后的核心开发者是一个影响比较强的组织，但比特生态存在明显的多方势力制衡。矿池、开发者、比特币大户之间互有强劲的博弈关系，不是说开发者推行什么我矿工就会无条件接受，如果提案过分的话，矿工和矿池都会直接反对。

这个点我觉得和以太坊不一样，像以太坊POW转POS、EIP-1159这些，当时都有很大争议，但以太坊基金会或者说Vitalik本人很大程度上只手遮天，这是有目共睹的。另一方面，以太坊生态现在非常庞大了，上面有非常多中心化发行的资产，像RWA、稳定币等等，一旦产生真正意义上的分叉，真正决定未来走向的是这些中心化资产的发行方。

所以无论主观还是客观上，以太坊生态里以EF为首的中心化势力都要比特币生态里各种组织的话语权强大得多。还有一点，就是比特币生态里没有特别统一的价值观，比如核心开发者更接近于比特币最大主义，抵制OP\_CAT或是铭文这种东西，希望比特币不要做太多改变；外围一点的开发者可能倾向于支持OP\_CAT的通过之类的。再往外一层，像闪电网络、RGB这些团队，相较于前两者更加倾向新鲜事物。再就是像我们这种，不但更愿意接受新鲜事物，还会主动求新求变。最后一层，则是把什么多签桥、EVM系二层全加进来了。

因为有了不同来历的形形色色的人，比特币生态的包容性非常好，不用担心某一层或者某一小搓人是错的，它们的错误会把整个生态带偏如何如何。这么多群人，只要有一群最终是对的就行。而以太坊的模式虽然在表面上走得更快，但比特币的模式走得更稳，不用担心某一小搓人的错误决定将整个生态带入深渊。所以从这个角度，我们非常看好比特币生态，因为它就像一个大熔炉一样具有强大的包容性和纠错能力。

再拿BTC二层举例，我看到你们的网站BTCEden上，汇总了各种各样不同思路的方案，有闪电网络、RGB这种客户端验证模式，还有侧链甚至是横跨以太坊和比特币的二层，总之百花齐放各显其能。而你再去看以太坊，Sharding没人做了，状态通道和Plasma也没人做了，几乎只有Rollup系的单一路线。所以我们当然更喜欢比特币生态，他更自由，更稳健。

CKB基金会也在尝试把决策变得更加去中心化。当然，我现在不在基金会里面，没有发言权，但是我可以看到更多的角色逐渐偏向社区化发展。CKB体量整体还比较小，对去中心化决策的要求还没那么强烈，大家对CKB的期待可能还是更快一点。但据我了解，CKB的核心决策人员是非常开放的，不会把过大的权力攥到自己手里，一定会找适合的时机完成去中心化。