RGB介绍

一句话概括，一个客户端验证在链下、数据储存在链下、合约代码在链下， 这些数据的锚定储存在链上，通过一次性seal来防止双花的layer2扩容协议。

个人感觉有点类似交易所的概念。
主要技术组成分为两部分：LNP/BP标准协议、RGB

LNP/BP

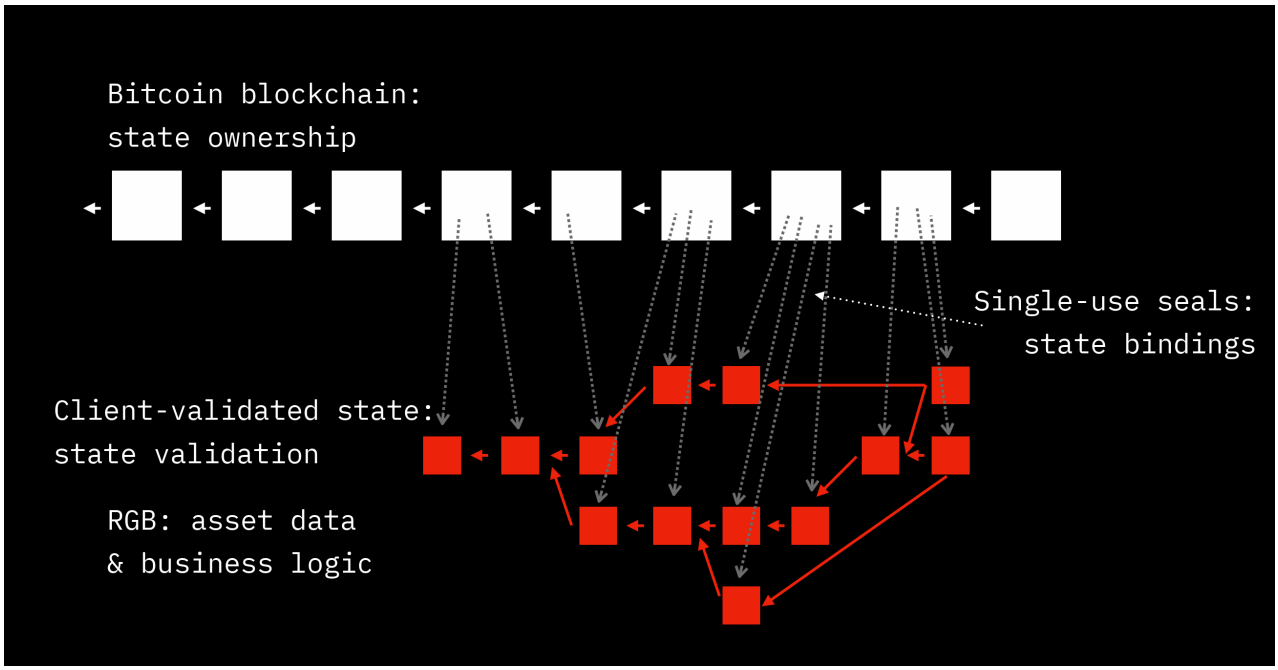
1. 承诺
2. RGB
3. LN协议

承诺

对于给定的消息msg Secp256k1 curve P* := {P1, P2, ..., Pn}, n > 0, 以及初始公钥P0 属于 P* 公共tag已知

1. lnpbp1_msg = SHA256("LNPBP1")| SHA256(tag) | msg
2. f = HMAC-SHA256(lnpbp1_msg, S*)
3. F = G * f
4. T = Po + F
   T = Po + G * HMAC-SHA256(SHA256("LNPBP1") | SHA256(tag) | msg, S*)

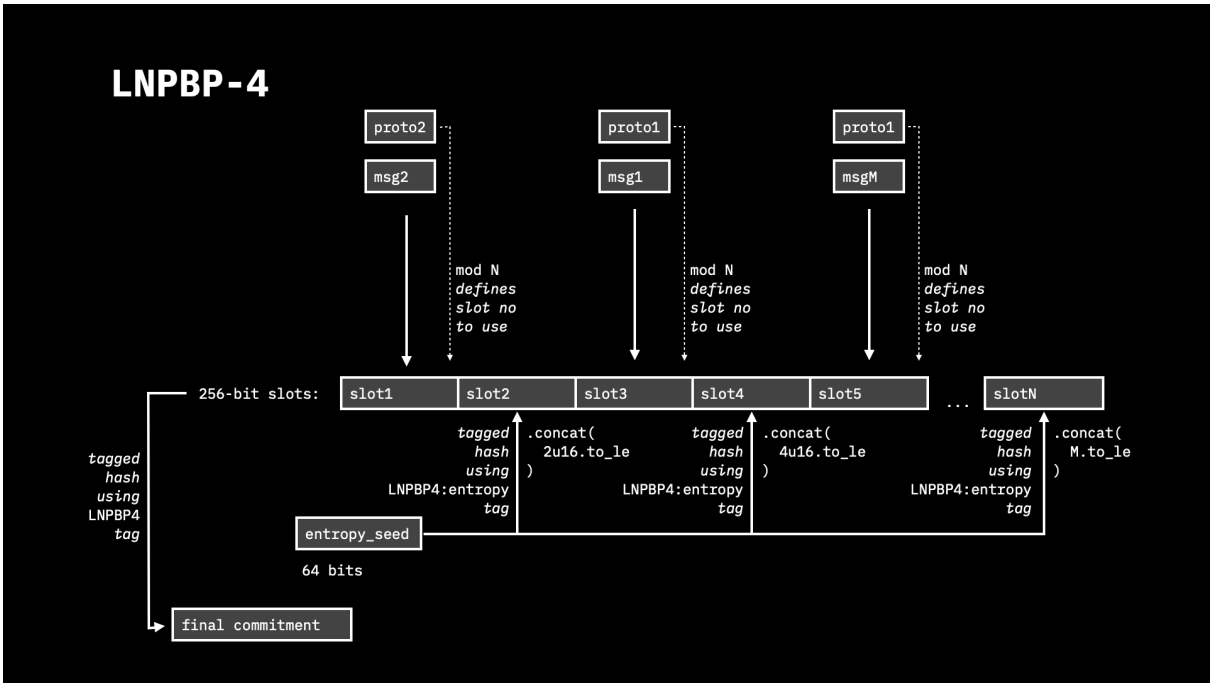
将承诺比特币化



1. Script
   目的是将承诺的算法变成bitcon适用的算法规范化。

2. Tx output
   用于确定交易的输出，方便作出承诺

3. Multi-protocol
   多协议适配

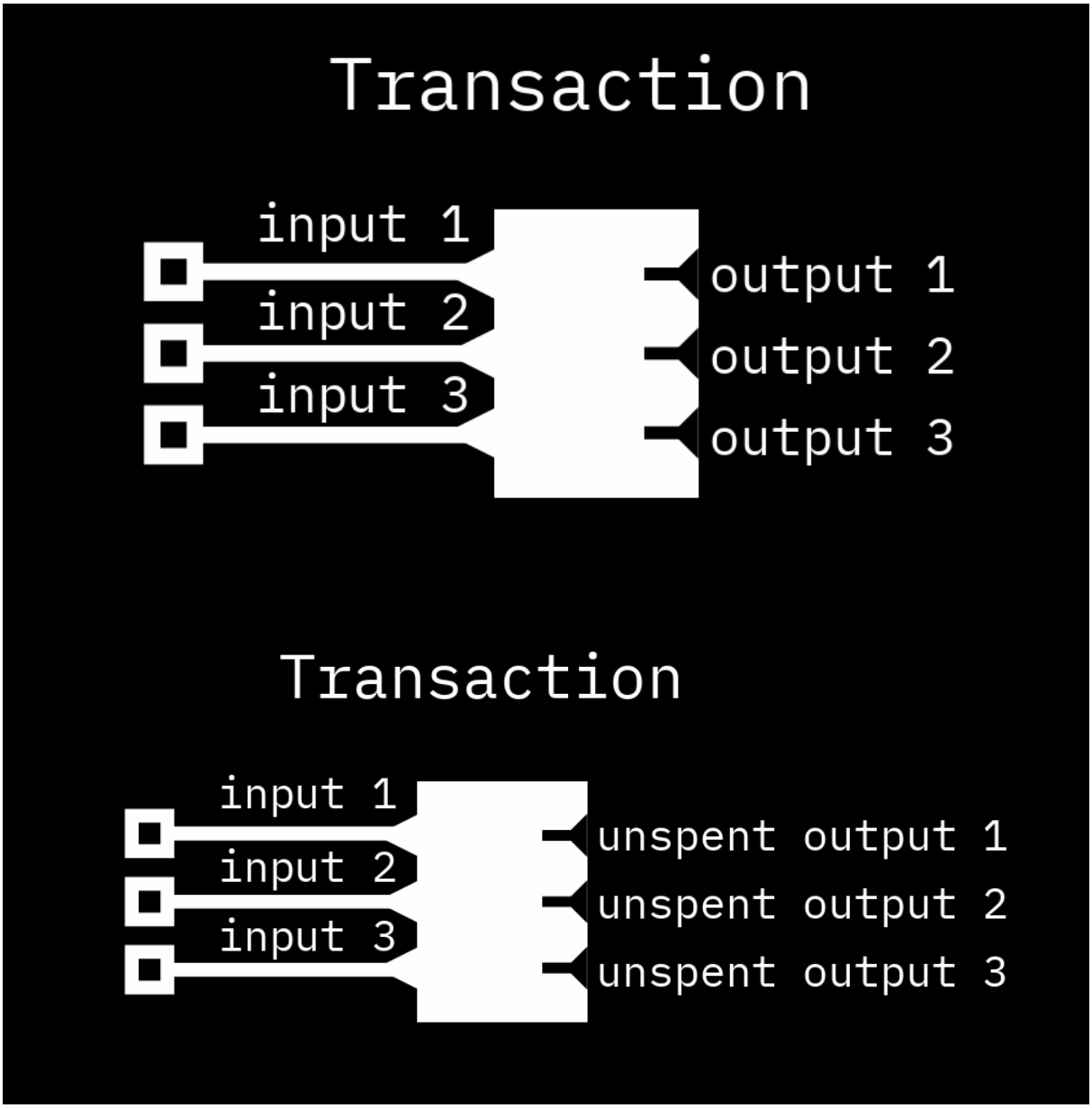


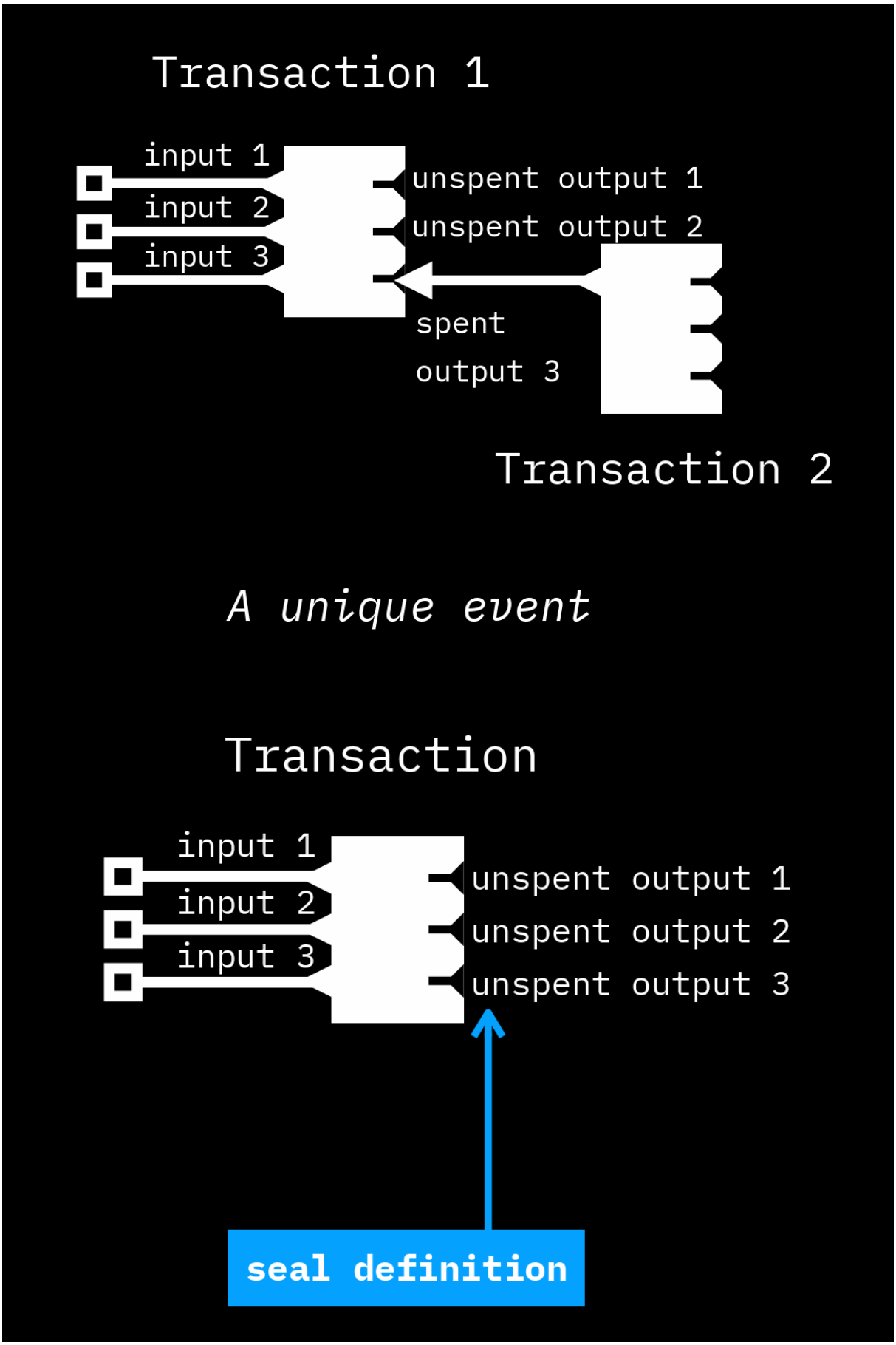
4. PayTweak
   多种协议可以通过构建特殊的数据结构“锚定” 并且提交交易的输入输出内容，来实现链下对应。

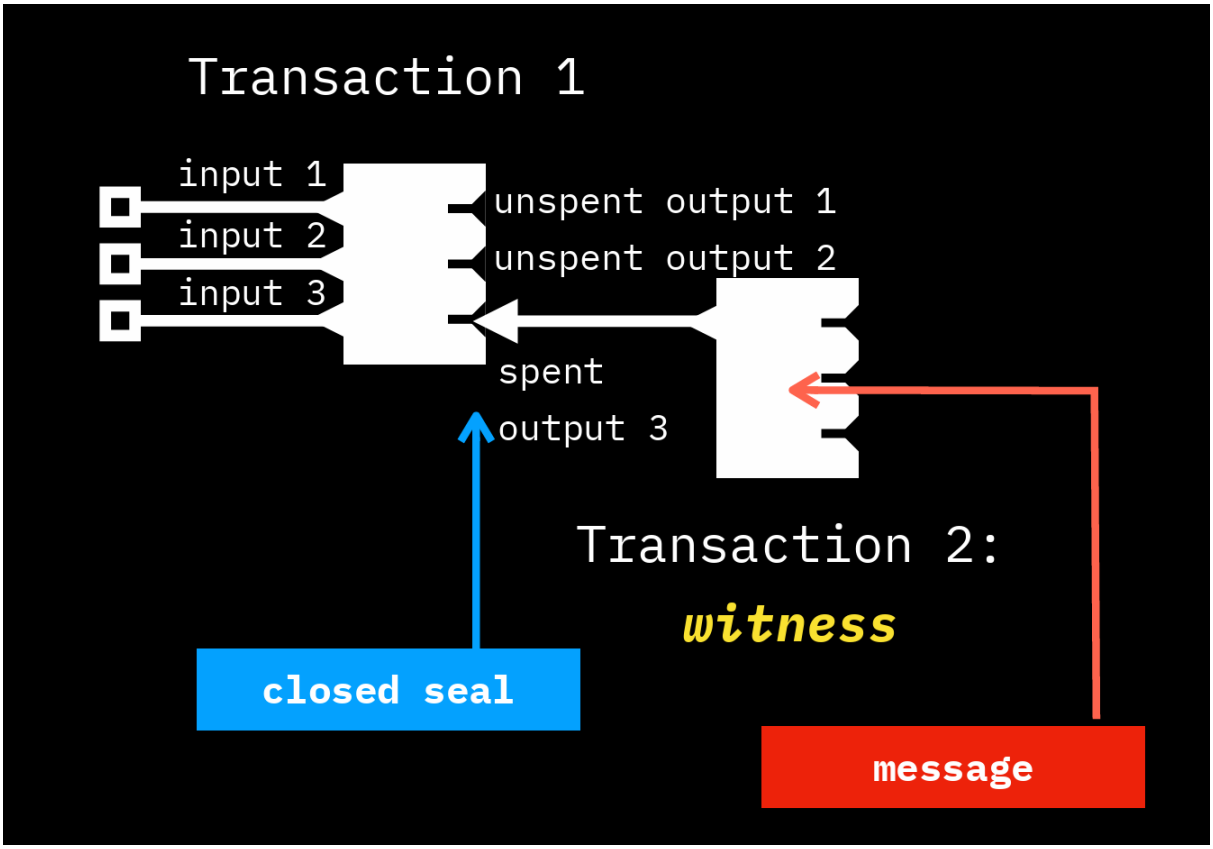
5. TapRet
   标准化到bitcon当中，将承诺放到taprooot script tree

6. Single-use-seals

7. TxO seals


Transaction
input 1
input 2
input 3
output 1
output 2
output 3
Transaction
input 1
input 2
input 3
unspent output 1
unspent output 2
unspent output 3


Transaction 1
input 1
input 2
input 3
unspent output 1
unspent output 2
spent
output 3
Transaction 2
A unique event
Transaction
input 1
input 2
input 3
unspent output 1
unspent output 2
unspent output 3
seal definition



Single-use-seals 防止双花

RGB

共识层

1. 客户端验证
   Single-use-seals 、 TapRet 提供链外数据 进行客户端验证。
2. AluVM
3. 合约

应用层

编写合约
与合约交互等
https://blackpaper.rgb.tech/application-layer/6.-writing-contracts.-scripting
(https://blackpaper.rgb.tech/application-layer/6.-writing-contracts.-scripting).

总结

RGB 很多技术可以被zk所取代，看他的代码也在逐渐更新，不过目前看来是起步阶段，至少他的LNP/BP协议目前的内容和ZK差距比较大没有引入zk相关的内容只是用了密码学相关的初级内容进行了实现。