

{ UDA // BTC }

原子交换

私密 · 点对点 · 无脚本

在比特币上

基于 RGB 0.11.1

Gideon Nweze

创始人

BitMask / DIBA 团队 · 技术论文 · bitmask-core v0.11.0-beta.10

摘要。一种纯粹点对点的比特币独特数字资产交换方式，将使卖方与买方无需经过交易所即可直接相互结算。预签名要约解决了其中一部分问题，但如果在交易完成之前仍需要可信的第三方来保管资金或资产，其主要优势就会丧失。

我们提出一种解决结算问题的方案，采用客户端验证和单笔比特币交易。卖方签署一份花费持有该资产之输出的要约。买方将该要约与一笔付款合并，在 tapret 输出中对这次转移作出承诺，然后广播。向卖方付款的同一笔交易同时完成资产的重新分配。系统本身只需要极简的结构：用于发现的订单簿，以及用于传递证明包的中继，二者都不持有资金或资产。卖方在发布后即可离开，并在结算时重新加入；资产历史保留在链下，由各参与方持有。

1. 引言

艺术品、产权凭证、票券和证书等独特资产的交易，仍然依赖于在交易完成之前代为保管资产、现金或二者兼有的平台。用比特币白皮书中的话说：“我们需要的是一种基于密码学证明而非信任的电子支付系统，使任何两个愿意的参与方无需可信的第三方即可直接相互交易。”

[1] 我们将这一原则应用于以 BTC 出售独特数字资产（UDA，即 RGB21 schema），并已在 bitmask-core 基础设施中实现 [2]。

2. 要约

“我们将电子货币定义为一串数字签名。” [1] 我们将要约定义为提前给出的一次签名。卖方构建一笔部分交易（PSBT v2 [4]）：它花费持有该资产的输出，添加一个返还输入金额并将承载承诺的宿主输出，再添加一个支付到全新地址的价格输出。该输入使用 SIGHASH_NONE | ANYONECANPAY 签名，因此无需任何一方在线即可完成交易。证明包、分片（shard）和一个盲化封印随要约一同传递。

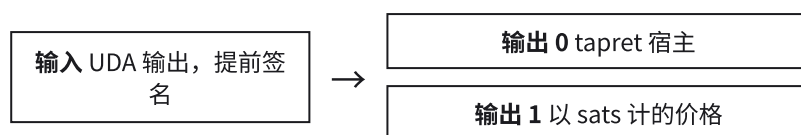


图 1. 要约：卖方的部分交易。

3. 封印与承诺

一份 RGB 资产被分配给一个一次性封印，该封印即一个比特币输出 [3]。花费该输出即关闭封印，花费交易则通过 tapret 承诺（Method::TapretFirst, [5]）对状态转换作出承诺。链上唯一的痕迹，是隐藏在 taproot 输出中的一个哈希，看起来与其他任何花费无异。事件的先后顺序由比特币链决定，而不是由各参与方决定。

4. 客户端验证

资产的历史不在链上。它以交付包（consignment）的形式随资产一同传递，交付包是由多个状态转换包构成的链，每个转换包都锚定在某笔交易中。买方在付款前，针对 esplora 解析器验证合约，并导入卖方的锚点。每一方都会验证自己收到的交付包。验证只消耗参与方已持有的数据。

5. 网络

运行这次交换的步骤如下：

- 1) 卖方签署要约并发布。
- 2) 买方获取该要约，验证其合约与历史。
- 3) 买方为出价备好资金：BTC 输入、找零和一张 RGB 发票。
- 4) 买方合并两份 PSBT，并检查价格输出是否保留。
- 5) 通过脚本绑定找到卖方的宿主输出，并构建 tapret 承诺。
- 6) 买方将交付包发布到中继，然后广播。
- 7) 记录撮合结果；卖方验证并登记该承诺。

“节点可以随时离开并重新加入网络” [1]。这里卖方在第 1 步之后离开，并在第 7 步重新加入。

6. 激励

买方承担价格以及固定的链上手续费，其他手续费模式一律拒绝。卖方收到以 sats 计的价格，并取回被花费输出的价值。

7. 同一输出上的其他资产

卖方的输出可能承载其他合约的分配。对每一项分配，要约都包含一个额外的分片，合并时会写入空白转换，把该分配重新指派到卖方的宿主输出。若任一额外资产为 RGB20，宿主将使用 RGB20 密钥链，使这些资产仍可由卖方花费。出售一项资产，不会使其他资产被困住。

8. 验证

“不运行完整的网络节点也可以验证支付。” [1] 同样，参与方只需要一个 esplora 端点和自己的 stock（本地合约库）：UTXO 与见证数据会被预取，合约会被验证，交易也通过同一个端点广播。

9. 价值的合并与拆分

“通常情况下，交易要么只有一个来自较大前序交易的输入，要么有多个输入以合并较小的金额，并且至多有两个输出：一个用于支付，另一个用于找零。” [1] 合并后的交易保持这一形态。输入按买方的在前、卖方的次之、其余在后的顺序排列。输出依次为卖方的宿主输出和价格输出，然后是买方的输出。宿主输出的脚本记录在要约中，若缺失则合并失败。

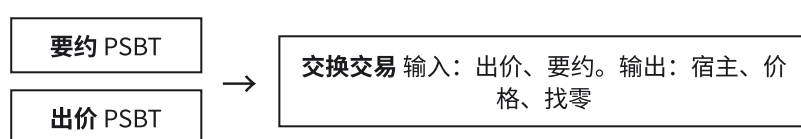


图 2. 两笔部分交易合并为一笔。

10. 隐私

仍然可以“在另一个环节阻断信息流：保持公钥匿名”来维护隐私 [1]。这里的阻断发生在链与状态之间。资产数据保留在链下，接收方由盲化封印指定，每个要约和每次出价都使用全新的派生密钥。链上只显示一笔带有 taproot 输出、不含任何资产数据的交易。共享的订单簿是另一个单独的环节，保存着交易记录。

11. 结论

“我们提出了一种不依赖信任的电子交易系统。” [1] 本文为独特资产提出了同样的方案。要约只需签署一次、合并一次，并在一笔比特币交易中结算，资产状态保持私密。

参考文献

- [1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.
- [2] DIBA Team, bitmask-core v0.11.0-beta.10, src/rgb.rs and src/rgb/swap.rs.
- [3] RGB protocol 0.11.1: rgb-ops, rgb-consensus, rgb-invoicing, rgb-psbt-utils.
- [4] BIP-174, Partially Signed Bitcoin Transaction Format; BIP-370, PSBT Version 2.
- [5] BIP-341, Taproot; BIP-86, Key Derivation for Single Key P2TR Outputs.