合约币(Counterparty)协议(2014/9/16 更新)

本文译自Counterparty的Github协议说明文档：https://github.com/PhantomPhreak/Counterparty

译者：申屠青春　深圳大学 ATR 国防科技重点实验室博士　新浪微博　@我看比特币

注意：本文可随意转发，请留下译者信息，如果觉得本文对你有用，请给译者捐赠，以便翻译更多比特币的核心资料。捐赠地址：1faVxBp2KmST98p3tJjx2MQP98JLLnF2Q

译者前言

比特币在国内已经众所周知，但是技术研究并未有效开展，大部分人处于知道和了解程度，目前比特圈中许多人对比特币能做什么，同样了解不多。一个重要原因是大多数比特币核心资料都是英文，很少有人能静心看完如此繁杂的英文资料。本人博士论文的研究方向是比特币，在研究其英文技术的同时，拟对一些重要资料进行翻译，让更多的圈内人对比特币有更多的理解。

本文涉及 Counterparty 协议，Counterparty 是比特币块链上的寄生应用，目前已经实现了众多技术创新点如燃烧证明、合约、去中心化 XCP 与 BTC 交易所、赌约或期货、资产或股份发行、分红等，对于一些想在比特币块链基础上有所创新的创业者来说，具有极高的借鉴意义。

正文

合约币是以合约币协议运行的全套金融工具，合约币协议建立在比特块链基础之上，把比特币块链当成可信的时间戳服务和可信的信息发布证明。

参考实现 counterpartyd，源代码：https://github.com/PhantomPhreak/counterpartyd

1 交易

每个合约币信息都包括以下特性：

- 一个源地址
- 一个目的地址
- 一定数量的比特币，从源代码发送到目的地址(如果目的地址存在的话)

- 以比特币计的费用，支付给挖到这个交易的矿工
- 最多 80 字节的数据，嵌入到比特币交易的结构化输出中(译者按：目前是指多签地址)。

每个承载着合约币交易的比特币交易有以下可能输出：一个目标输出、0 字节或更多字节的数据输出、可选的找零输出，在第一个数据输出之前的第一个输出是目标输出，找零输出(在数据输出之后的输出)对合约币来说不重要，所有数据输出必须在直接继承中出现。

为了方便区分，每个合约币交易的数据区域都以 UTF-8 格式的‘CNTRPRTY’打头，这个字符串已经足够长，因而很难把合约币的交易和在伪随机数的比特币交易搞混。在测试情况下(例如：在任何块链中使用 TESTCOIN 合约币网络)，这个字符串是“XX”。

合约币的数据可以以三种不同类型的输出来存贮，或者以这三种类型的混合来存贮。多签名数据输出，是 1-of-2 输出，第一个公钥是发送者的，因而输出的币值可以赎回，存贮第二个公钥的空间可以用来存贮编码的数据，前缀是长度字节，用 0 来填充后面的无数据区域。OP_RETURN 数据输出格式 pay-to-pubkeyhash。

字节串“CNTRPRTY”之后的四个字节说明了目标地址是否存在、比特币交易费用多少和交易的比特币数量(根据合约消息类型不同而不同)。其他的数据根据消息类型有不同的格式，参考源代码。

另外，每个合约币交易必须有一个明确且唯一的源地址，在含有合约币交易的比特币交易中，所有输入都必须一致-在比特币交易中的资金唯一源地址，就是合约币交易的源地址。

合约币交易的源和目的地址，就是比特币地址，任何比特币地址可以收到任何合约币的资产(如果该地址有资产的话，也可以向外发送资产)。

所有信息按照顺序解析，一次一个，忽略区块边界。

订单、赌约，在区块的结尾结束匹配订单和赌约。

- 目前仅支持 Pay-to-Pubkey-Hash

2 非合约币交易

counterpartyd 支持构建两种类型的交易：

- BTC 发送
- 以 BTC 发送合约币的资产分红

这两种交易不包含数据区，对于后者，能使用多个“目标”输出。

3 内存池交易

块索引总是为=9999999 (config.MEMPOOL_BLOCK_INDEX)

DB 的变化不会跨会话保存。

不匹配订单或赌约。

4 资产

除 BTC 和 XCP 以外的所有资产有如下特性：

- Asset name 资产名称
- Asset ID 资产 ID
- Description 描述
- Divisiblity 可分性
- Callability 可赎回
- Call date (if callable)赎回日期(如果是可赎回的)
- Call price (if callable)赎回价格(如果是可赎回的)

资产名称是大写 ASCII 字符串，当编码成十进制整数时，大于 26^3 小于或等于 256^8。所有资产名称，除了“BTC”和“XCP”，必须至少有 4 字节长，而且不能以字符“A”开头。这样，某些 13 字节的资产名称是有效的，但是 14 字节的就不行。

资产可以是可分割的或者不可分割的，可分割资产可以分成 8 个十进制的位置。资产可以有描述，可以随时改变。

资产可以是“可赎回的”，可赎回资产在赎回期之后，可以被现在的发行者，以赎回价格(以 XCP 为单位)强制“赎回”，赎回价格设置成该资产首次发行的价格。

可赎回资产可以在赎回日期之后赎回，该赎回日期是在块链中的一个区块中第一次定义的时间。

赎回价格指定为 6 个十制数的精度，是 XCP 与该资产(不是 satoshis)的最小单位的比率。

5 数量，价格和分片

- 最大整数
- oversend, overbet, overorder

not btcpay, callback (impossible, because of rounding), issuance (fragile!), dividend (?!)

(译者注：这段不知道具体意思，不翻译了)

6 过期

- 最大过期时间
- 在区块开始(在交易被解析之前)

6 交易状态

当订单和赌约的 give_remaining, get_remaining,wager_remaining, counterwager_remaining, fee_provide_remaining 或 fee_required_remaining 小于等于 0 时，订单和赌约的状态将被设为 filled。

因为当订单匹配成功，但 BTC 支付过期时，订单有可能不被满足，所以这种时候就保留 open 状态。

7 消息类型

- Send 发送
- Order 订单
- BTCPay BTC 支付
- Issue 发行
- Broadcast 广播
- Bet 赌约
- Dividend 分红
- Burn 燃烧
- Cancel 取消
- Callback 回调

7.1Send 发送

发送是指从源地址发送任何合约币资产到目标地址，如果该消息被解析(以交易顺序)

时，发送者还没有足够的资产数量，该发送消息只能部分满足。

counterpartyd 支持发送比特币，这里不使用任何数据输出。

7.2Order 订单

订单是指给定某种资产的特定数量，要得到其他特定数量的资产。“买单”和“卖单”之间没有本质差别。在订单解析时，被卖出的资产通常马上被托管。也就是说，如果有人想用 1 个 XCP 换 2 个 BTC，一旦他发布了这个订单，他的 XCP 帐号马上被减去 1 个 XCP。

当订单在块链中可见时，协议试图去撮合它和另一个以前见过的开放订单。两个被撮合成功的订单称为“订单对”，如果订单对中的任何一个订单包含比特币，那这个订单对会被指定“待处理”状态，直到必要的 BTCPay 交易发布；如果订单对中的订单没有包含比特币，这个交易将立即完成，并且以协议自身指定的地址形成新的收支平衡。

所有订单都是定价单：询价指定了一个人想付出和得到的比率，订单会匹配定价以下的最优价格，订单对就是按照这个价格撮合的。这就是说，如果有个开放订单以 0.11XCP/每份资产卖出，第二个卖单以 0.12XCP/每份资产卖出，第三个卖单以 0.145XCP/每份资产卖出，然后有一个新订单要以 0.14XCP/每份资产的价格买入，将会先匹配第一个卖单，XCP 和 BTC 将会以 0.11XCP/ASST 的价格成交，如果还有剩余买单，则再匹配第二个卖单。如果两个卖单的价格相同，则以时间顺序成交。

所有订单允许部分执行，这儿的订单并非要么完全成交，要么不成交。在前一个例子中，如果购买比特币的一方想买的数量多于第一个卖单的数量，买单剩余未成交的数量会由后面的现存卖单来满足。在所有可能的订单对撮合完后，当前买单被列为开放订单(如果还有数量未被满足的话)，如果存在多个价格相同的开放买单，则订单将按照时间顺序撮合。

开放订单被用户发布后，会在用户定义的区块数量后过期，当订单过期，所有担保的资金会返回订单发布的那一方。

等待比特币支付的订单对将在 20 个区块(译者按：以前是 10 个区块)后过期，其中的订单会重新发布。

一般地，不会存在虚假交易，因为每一方提供的资产都存贮在合约处，然后，担保比特币是不可能的，因而那些想购买比特币的人会要求只匹配有向比特币矿工支付网络费用的交易。另一方面，当创建订单售出比特币时，用户可以支付任意他愿意支付的费用，部分订单仅支付部分费用。这些费用对应代码中的 fee_required 和 fee_provided，当涉及 BTC 的订单

匹配时(或过期)，这些费用(必须的和提供的)，以订单匹配部分的比例变成负债(有些重新发布)。也就是说，如果一个订单卖出 1BTC，fee_provided 是 0.01BTC(1%)，订单初始匹配了 0.5BTC，fee_provided_remaining 将变成 0.005。然而，当 BTC 支付失败时，提供的费用不用返还，否则它们的反炒作就会失效。

用比特币支付来关闭那些等待 BTCPay 消息的订单对。在 BTCPay 消息的数据区中，存贮着两个 HASH 串连接而成的字节串，而这两个 HASH 串则由订单对中的两个订单 HASH 生成的。

7.3Issue 发行

资产可以以发行消息类型发行：用户指定名称和数量，协议计入它相应的地址。资产名称必须是唯一或者以前被相同地址发行过的。当重新发行一个资产，就是说，对已经发行的资产进行增发，发行的资产名称、可分割性和发布地址必须匹配。

对某个已经存在的资产进行增发，这个权利可以转移给别的地址。

资产可以被不可逆地锁定，防止进行增发，保证资产拥有者免受通涨风险。要锁定资产，可以把描述设为“LOCK”(大小写不敏感)。

任何非 0 数量的发行，也就是说，发行不仅仅改变资产描述，还包括债务(和取消发行)，需要 0.5XCP 的费用。

7.4Broadcast 广播

广播消息发布文本或数字信息，并且附带一个时间戳，作为系列广播的一部分，被称为“反馈”。一个反馈和一个地址相联系：从给定地址过来的任何广播，都是该地址的反馈的一部分。一个反馈的时间戳必须单向增加。

赌注以数字形式在反馈中下注，这个数值可以是货币的价格，或者可以是对未来事件的离散可能输出的一部分描述。例如：有人可能以文本这么描述：“US QE on 2014-01-01: dec=1, const=2, inc=3”，并且宣布结果“US QE on 2014-01-01: decrease!”和数值 1，更为复杂的赌约可以以非块链的方式发布。

发布内容为文本字符串“LOCK”(大小写不敏感)的单个广播可以锁定反馈，阻止它成为以后的广播源地址，同时也阻止它成为任意新赌约的主题。(如果反馈被锁定，如果还有

开放的或未解决的赌约与之相关，那些赌约或赌约对会无损害地过期)

反馈以发布它的地址来识别。

广播-2 的数值会取消所有在反馈中开放赌约，广播-3 取消所有反馈中正在处理的赌约对。(这个等效于在截止日增等待两周)。广播任何一个负值将被赌约所忽略，但他们将更新广播时间。

7.5Bets 赌约

目前有两种赌约，第一种是打赌一个特定反馈会等于(或者不等于)一个特定的数值-目标值-在最后期限。第二种是一个合同，所不同的是有一个特定结算日期。简单的等于/不等于赌约，和牛/熊差价合约都把各自的赌注放到撮合成功的担保契约中，当他们依据的反馈通过最后期限，赌约就解决了。事实上差价合约可能是被强行结算的，当反馈值变化剧烈时，保证金耗尽被强行平仓。

差价合约可以用杠杆操作，它们的杠杆水平是 5040 等于一个单位，以整数保存。5040 的杠杆水平意味着保证金杠杆应该是 1：1，10080 的水平意味着反馈每增加一点，牛/熊合同的数值要增加(减少)2 点。

差价合约没有目标值，等于/不等于赌约不能用杠杆。然而，为了让两个赌注能被撮合，他们的杠杆水平、时间期限和目标值都必须相同，否则，他们会以订单的形式撮合，除了赌约的赔率与订单价格是反相关的(赔率=保证金/庄家保证金)的情况，如果有可能，每个赌约都会以尽可能地高的赔率撮合到开放赌约。

目标值必须非负，赌约对(合约)不受-1 的广播值所影响。

赌约的最后期限不能晚于他们指定反馈的最后一个广播的时间戳。

赌约的过期与订单相同，例如：过了特定的区块数量后。赌约对在 2016 个区块后，当看见一个区块的时间戳在赌约的最后期限之后过期，

赌约费用是初始保证费用的比例，这部分并非赌约收入。它们将从初始保证金中扣除，并非加到其保证金上。

- 因为区块时间的存在，以及交易在块链中被订单化这种非确定性方式，所有合同必须非增量解决，但是涉及的资金必须马上放入担保契约，而且必须有解决日期。否则，有人看到价格下跌了，把要被扣除的资金隐藏起来。

反馈费用从最后交易金额中扣除。

7.6Dividends 分红

分红支付是以一定比例为基准，支付一定数量的 XCP 或 BTC 给每一位特定资产(除 BTC 和 XCP)的拥有者。以分红收入为目的的资产可以是可分割的或不可分割的。任何资产的分红支付可以来源于任意地址。用来支付分红的资产，和股票拥有者收到分红支付的资产，可以是一样的。比特币分红支付不使用合约币协议，因而会比其他分红支付更多费用。

7.7Burn 燃烧

Counterparty 的货币"XCP"，在一段特定时间内使用燃烧消息类型把比特币"燃烧"成矿工费用，以完成 XCP 的初始化。每个比特币获得的 XCP 数量，可以通过以下公式计算：

XCP_EARNED = BTC_BURNED * (1000 * (1 + .5 * ((END_BLOCK - CURRENT_BLOCK) / (END_BLOCK - START_BLOCK))

END_BLOCK 是燃烧阶段结束时的区块(block #283810)，START_BLOCK 是燃烧阶段开始时的区块(block #278310)，燃烧得越早，价格越好，在 1000-1500 XCP/BTC。

燃烧消息有存贮在 OP_RETURN 输出中的精准字符串'ProofOfBurn'作为识别。

- 新数据-更少燃烧
- 燃烧期已经结束

7.8Cancel 取消

开放订单可以被取消，取消操作是不能被取消的。

一个取消消息仅包括比特币交易的 HASH，该比特币交易包含将被取消的订单或赌约，只有下单的地址才能取消订单。

当等待 BTCpay 消息时，不能取消订单对(如果买入 BTC，不公平；如果卖出，不必要)

7.9Callback 回调

Callback 目前在合约币的主网中是被禁用的，只在逻辑上被解析，正在不断修和测试。