The Public Coin
一个基于众筹而生的对等网络

摘要。 基于比特币和智能合约而生的带来加密货币。公平货币分配和安全性的各种改进，此网络能够促进全球众筹项目的优化。

简介

比特币，已经成为一种流行的数字货币，备受全球的关注和交易，并吸引大量用户。自 2009 年它成立以来，比特币已经迅速成为主流，而且越来越多商户使用。在零售情况下接受比特币的主要问题是等待网络确认的交易有效时间，虽然支付公司已经创建了允许供应商进行零确认交易的方法，但这些交易解决方案都必须信赖可靠的交易对手来处理确认交易。

公众币（TPC）是一个基于对等网络的众筹网络，具有其他虚拟货币如比特币的优势并附加各种改进，例如加速网络交易确认机制（ANTCM）和渐进式货币分布曲线。 TPC 项目认为，在备受比特币多年的技术安全基础下，POW 证明型设计完全解决了早期验证的网络安全性和网络认证集中问题，同时能够避免货币分配制度导致资金日益集中的问题。因此，TPC 是第一个无论在技术，安全性，成本效益和分散程度上带可持续性的货币。
在 TPC 可扩展的基础之上，智能合约层很容易就能够扩展实现，因为 TPC 是分散的，他能够成为公正的项目资金众筹网络，让 TPC 用家能够在全世界筹集用于创新发明的服务。传统的集资需要 5-10% 的佣金，在 TPC，合约和资金由 TPC 网络的明细所约束，因此，手续费及佣金全免。在其他數字貨幣上，这取决于参与交易方，该项目使用的服务提供商但在 TPC，用户和项目资金发行人不会受到支付系统的交易对手风险所影响。一旦资金项目达标，满足资金将立即被释放。

交易

TPC 交易消息具有以下组件：

- 源地址
- 目的地地址（可选）
- 从源发送至目的地 TPC 量，如果存在的话。
- 一次收费，在 TPC 网络支付给 TPC 矿工。
- 一些“数据”，嵌入在专门构造的交易输出。

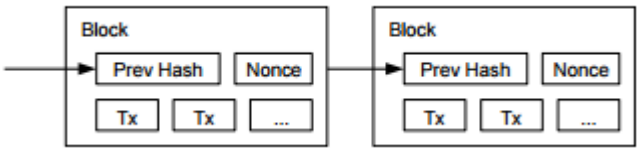
每个 TPC 可选包含以下数据：

- 零个或多个目标输出，
- 零以个或多个数据输出，及可选的变化输出。

所有数据输出遵循所有目标输出。更改输出（最后一个数据输出后输出）没有意义。

确认和验证

我们定义币数作为电子签名链。任何未成交输出（UTXO）可以通过相应地址的私有密钥持有人签名并使用，通过发出一个数字签名到网络。网络交易确认机制（ANTCM）利用确认网络上矿工交易的存储池。当数字签名由节点发出，它将会以点对点方式传播网络。由于 TPC 的缩短确认时间设计，交易处理比传统基于链的交易记录网络快 4 倍。



当交易由矿工确认，确认的结果会点对点的立即传播到网络中。

分散的资金

由于 TPC 的高效，安全的网络设计，网络可以利用项目资金机制是分散的追加。我们把项目作为网络资产集资的项目将赋予用户产品、特权、分成、股权等。除了 TPC 所有的资产都具有以下属性：

- 资产名称
- 资产 ID
- 说明
- 可除性
- 可回溯
- 赎回日期（如果可赎回）
- 收回价（如果可赎回）（非负）
- 可再次发行

新注册的资产名会可以是任一的 4 至 12 大写拉丁字符（含）不与'A'开始，或 26 之间^ 12

+ 1 和 256 ^ 8（含）的整数（唯一）的字符串，带有前缀'A'。字母的资产名会进行一次性发行费用 0.5 TPC 的和数字资产的名称将免费提供。 “TPC”是唯一的三个字符的资产名。资产名称可以是：BBBB，A100000000000000000。

资产可以是可分或不可分割的，分割财产是可分到小数点后 7 个位数。资产还配备了描述，这可能是高达 52 个单字节字符，并随时更新。

资金类型

最基本类型的资产必须注明：

- 是谁发出它（source）
- 资产代码（asset）
- 发行量（quantity）
- 描述（description）

发行過多的 资产是有可能的，但是，在任一时间，只能有一个地址发出 资产。换言之，TPC 协议允许 source 传输发行任一资产的权利。此外，资产也可以被锁定，因此有可能成为它没有再发行。一个说明，必须包含，即使描述只是一个空字符串; 资产的语法 *没有描述* 是 description=“”。

除了创造了最基本的资产，也可能使资产要么整除或调用。如果资产，可依其初发制成整除（或可调用）时，它必须总是整除（或可调用）与此后每发行。可分割的用户创建的资产一样，比特币和 TPC，可分割多达 7 位小数。可调用资产是从它的拥有者的资产，其中发行者可以回溯（即回购），而日期（呼叫日期）和回收价格必须在发行时指定。

智能合約众筹應用

通过整合以太网络的整个智能合約平台，TPC 的用户能够编写智能合約到 TPC 区块链，而完全去中心化，并不依賴單一用戶的信任，而是整個網絡的驗證。

TPC 合同语言是以太网与以下未成年人的不兼容性除外完全兼容：

- 涉两个 EVM 的操作码（COINBASE 和 GASLIMIT）被拆除。
- 新 ASSET_BALANCE 操作码可用于获取本地交易对手的资产和 BTC 的平衡。它有两个输入端（地址和 ASSET_ID），并返回一个值（地址在资产负债命名）。它具有相同的 gas 成本 BALANCE（只着眼于 XCP）。
- 新的发送操作码可用于发送本地交易对方的资产交易对手（比特币）地址。 SEND 具有三个输入（地址，数量，ASSET_ID），并且没有输出;它具有相同的成本 CALL。

TPC 合同的基本费用结构是和以太网非常相似的。不同的计算或存储操作将收取不同的费用相关联，以防止系统被滥用。合同执行费将只在 TPC，TPCX 的本地货币（这是不可能为他们在比特币支付）支付。合同系统将与现有的 TPC 资产系统和分布式交换完全兼容。收费系统交易对手合同的经济是必然的以太网的相当不同的，仅仅是因为没有对手矿工。所有的对手节点将执行所有的合同，这将是 TPC 的接收的费用执行的持有人。使这笔款项的最简单，最可靠的方法将就是把费用取消，从而减少 TPC 的供应量，就相当于把费用按 TPC 持有人之 TPC 數量按付給所有 TPC 持有人。
和以太网不同的是，费用将不是恒定值，而是 TPC 的总现存量的分数，所以没有计算量将耗尽 TPC 的供应并把它打入负值：TPC 的整除保证了網絡中永遠都存在足够的 TPC。