BitcoinX—彩色币 白皮书

[**Really**](http://www.8btc.com/author/58)**2013-09-05 16:32 发布在**[**区块链**](http://www.8btc.com/blockchain)**,**[**比特币**](http://www.8btc.com/bitcoin)[**2**](http://www.8btc.com/bitcoinx-colored-coin#comment)**15496**

[](http://7fvhfe.com1.z0.glb.clouddn.com/%2540%252F%2F/wp-content/uploads/2013/08/bitcoin-illo.jpg)

作者：Leo (liorhakim@mail.com)、Yoni (yoni.assia@gmail.com)、Meni (menirosenfeld @ gmail.com)

翻译：Really

**摘要**

比特币是世界上第一个去中性化的数字货币，用加密令牌可以轻松实现存储和转移，用一个点对点的网络承载信息，对同步数据进行散列处理来防止双重支付，和强有力的脚本处理系统来判别令牌的所有权。不断成长的技术和商业基础支持着比特币的发展。

比特币被设计成一个中性的交换媒介，它是可替代的。尽管如此，通过仔细跟踪一些特定比特币的来龙去脉，可以将它们与其他的比特币区分开来，这些特定比特币就叫作彩色币。它们具有一些特殊的属性，比如支持代理或聚集点 ，从而具有与比特币面值无关的价值。彩色币可以用作替代货币、商品证书、智能财产以及其他金融工具，如股票和债券等。

彩色币本身就是比特币，存储和转移不需要第三方，可以利用已经存在的比特币的基础，因此彩色币可以为现实世界中难以通过传统方法去中心化的事物铺平道路。本文将要讨论彩色币的实现细则及他们的用途。

**背景**

比特币的点对点支付网络已经被确认是安全、稳定和自由的在账户间转移价值的工具。比特币网络协议层本身是安全和稳定的，比特币生态系统的网络服务提供商被黑客攻击过多次，这损害了比特币的声誉和交换价值。

基本的技术和货币的价值的关联导致人们认为技术不可靠，价值如浮云。

**概述**

BitcoinX的理念是在技术上将比特币网络从其货币价值中抽离出来，用比特币网络明确交易并避免双重支付。

BitcoinX的目标是在比特币网络的上层便捷地创造新货币。

**概念**

***创世交易***

这个理念是通过创世交易创建新货币。

创世交易里有曾经转移进来的一定数量的比特币。这些比特币将会用来创建新货币的价值。

新货币起源于比特币被转移进去的那个地址，这个地址将控制新货币的初始分配。

我们将创建新货币的轻客户端，用一个特殊的方法对新货币进行记账。

首先找到那些发送地址来自创始交易的平台地址，然后检查每一个交易的交易记录确认该交易是否来源于创世交易。

如果我们将创世交易的金额乘以一个新货币的初始稀释系数，我们就得到了用户所拥有的新货币的金额。比如：用0.00001BTC = 1 新货币。新货币客户端的分布创建了一个围绕特别创世交易的社区。这将这些彩色币和其他所有的比特币区分出来，因此这个使用比特币基础设施的在比特币网络上层的mini-eco系统将拥有浮动的价值。

***彩色币***

彩色币是在历史上的创世交易里面被转移过的比特币。因为所有的比特币交易记录被保存在 block chain里面，所以可以查询每一个比特币是否被染色。（染色的意思是这个比特币曾经的一次交易记录发生在创世交易里）  
1、因为这些彩色币本身就是比特币，所以彩色币可以通过比特币系统从一个地址转移到另外一个地址。  
2、因为我们有一种方法去区分比一般比特币更稀有的彩色币，因此彩色币的价值会基于比特币的价值以及对彩色币的需求而变化。

***初始分布***

新货币初创的时候，所有该货币的价值归属于一个单独的个人或团队；最后的分布是所有的价值从创始者转移给所有的客户。这两个阶段的过程就是货币的分布。

当初始分布完成后，创始者将不再经济中扮演中心的角色，客户完全按照他们认为适合的方式管理他们的经济。

在初始分布阶段，新货币能获得客户的信任，并在经济中创建价值分布的结构。

***分布算法***

分布算法是创始者选择的释放他所持有的货币到经济实体的方法。举一个简单的例子，为你所认识的人创造一种货币并平均分配给大家。首先这些人先安装客户端，然后用客户端将自己的地址发红给货币创造者，然后货币创造者通过创世交易将初始货币数量等分成等量的BTC发送给大家。当所有人收到自己的那一份，创始者手里的比特币都发送光，新货币就完成了在客户之间的等量分布。

现实中，创始者既不知道新货币将有多少账户数量，也不可能知道哪些人愿意参与进他的经济体。某种程度上，他可以创建并执行一些邀请机制，在这种机制作用下每一个新的潜在用户可能邀请更多的客户参与进来。

这些将对社交网络身份验证、社交图谱蔓延、担保系统、短信认证、独一无二的侵入保护系统、实物认证等等的发展大有帮助。这些方法可以用来在初始分布中最大限度的减少欺诈。

另外一个可能的方法是每一个邀请要消耗新用户一定量的比特币，来以此建立激励，避免人为操纵eco系统。

**结构体系**

目前看来bitcoinJS这个项目有一个更好的分离的实体来集成和建设轻客户端，轻客户端可以让客户不用在电脑上安装任何专用软件的情况下轻松完成交易的签约。

理念是在节点-通道的应用程序编程接口创建另外一个协议层，通过创世交易来获取账目余额。

**要求**

概念验证的轻型货币客户端

查询余额

应用程序接口（API）: 获取余额(比特币地址，创世交易)

发送货币

要能在客户端中签约交易并发送到出口节点

在客户端中生成新地址

最好有交易记录

**路线图**

拥有安全的分割关键架构

密码保护交易

创建自定义货币模式 (定义创世交易, 生成客户端)

**备忘录**  
交易机制

追踪区块链的基准数据库

思考其扩展性

思考费用模型

理解钱包（私匙）存储的地方

**最近的进展**

序决策逻辑下的弱着色概述及探讨  
[https://docs.google.com/document/d/1pOaWe1fWdcUUKdyXz3rMWQneGLfTg89QaIBkS91nngE/edit#](https://docs.google.com/document/d/1pOaWe1fWdcUUKdyXz3rMWQneGLfTg89QaIBkS91nngE/edit)

Alex的序决策逻辑下的弱着色理论: <https://github.com/killerstorm/colored-coin-tools/blob/master/colors.md>

Alex还建立了一个支持彩色币的 BitcoinArmory 客户端（作者已经声称放弃，并开发新客户端）  
<https://github.com/etotheipi/BitcoinArmory>

一个在bitcoinjs上实现序决策逻辑下的弱着色的chrome浏览器插件。  
<https://github.com/0i0/bitcoinjs-color>  
<https://github.com/0i0/bitcolor-chrome-ex>

围绕着比特币协议层上的多种货币的成长型社区网站  
[http://www.bitcoinx.org](http://www.bitcoinx.org/)

本文为Really独立翻译，欢迎转载，转载请遵循“署名-非商业使用”的共同创作协议。