木币：一种为长寿命和稳定性而建立的点对点电子货币 V1.0

Funkenstein the Dwarf

2014年10月31日

摘要：

我们在这里概述木币的设计考虑和实施，特别是与其他加密货币相区别的部分。木币是一种非常像比特币的加密货币。然而，比特币的设计是明确地将一种不可再生资源（黄金）做成了模型。对于木币，我们更加密切地将可持续资源做成模型。特别是木币可以避免比特币释放模型中时间的不对称性，最大限度地激励货币的参与和延长货币的使用寿命。我们的解决方案能使货币供应量成对数增长。此外，我们概述了在核心协议中两个其他更改后的设计考虑：使用Skein哈希函数进行挖掘，并利用椭圆曲线数字签名算法（ECDSA）的X9_prime256v1曲线来确保数字所有权。

简介：

六年前，伟大的奇才中本聪（Satoshi Nakamoto），通过宣传一个公开的加密货币（比特币Bitcoin[中本（Nakamoto），2008]）中首次实施的工作算法的证明，摆脱了伪造者的控制，传到了中土世界。我们目前的工作，木币是一种试验性的加密货币，它与比特币的方式非常相近，在代码库中分享了比特币和两个它的接班人：莱特币Litecoin和夸克Quark。木币的目标是采取很长远的视点，设计出一种即使在非常遥远的未来仍然切实可行且长久稳定的货币。

发布时间表：

对于金融应用和加密货币的稳定性至关重要的是收益时间表或者发布时间表。 这也被称为货币供给通货膨胀时间表。使用公共的加密货币，这个时间表不是私人的或随意的，而是提前计划的，并且被所有参与者验证和审核（监管）。中本聪（Satoshi Nakamoto）选择了一种非常粗糙地模拟不可再生资源开采的模型。每个区块都会给出固定不变的数量，然后在固定数量的区块（210000个区块或者接近4年的比特币经典版）之后，这个数量将被削减一半。这可以写成一个几何级数：

$$R_n = \frac{k}{2^n} \quad (1)$$

这里Rn是指在一些时间步骤n的收益，k是初始常数（比特币经典版k=50）。

这是数学上通用语，称之为等比级数，其总和随着n的增加而迅速收敛。这样的 结果是，在最初的四年之后，有一半的比特币被释放出来。此外，在不久的将来，如果每个块的收益接近零的时候，进一步的挖掘只有通过交易费来激

励。 目前尚不清楚比特币和其他加密货币在这个极限情况下的表现。 问题是执行单个区块花费双倍的成本和挖掘收益成比例。

正是这些特性，我们希望用一个对数发行货币来进行改善。对于木币，我们采用调和级数来替代等比级数，其中的收益由下式给出：

$$R_n = \frac{k}{n} \qquad (2)$$

在这种情况下，一个很直接的差异就是这个数列的总和是不会收敛的。 虽然在理论上这意味着无限的货币供应量，但是因为我们受到1satoshi（10^{-8} LOG）的最小可能收益的制约，所以也会有最终的限制。

然而，调和级数的增长非常缓慢。当Rn=10^{-8}时，才到达最终收益的时间。对于木币，我们选择了k=1000000，我们知道当区块数n=10^{14}的时候才出现最终的LOG satoshi，那已经接近了大家说的朱利安3.8亿年。最大的货币供应量将在这一年达到，刚刚超过27,625,814LOG。

比特币在四年内发布了一半BTC，我们预计在朱利安2305年将会发布一半的LOG。

当任意区块n时的总LOG货币供应量是通过将之前所有的区块收益相加来确定的：

$$S_n = \sum_{100}^{n} \frac{k}{n} \approx k \cdot \log(n+\gamma) - F \qquad (3)$$

其中的近似值是来自伟大奇才欧拉。这里的γ是欧拉-马歇罗尼常数～0.577，log是自然对数。F代表森林的大小，这些木材是由那些未添加到供应量中的最初区块构成的：

$$F = \sum_{0}^{100} \frac{k}{n} = 5,187,377 \qquad (4)$$

引入森林是为了消除早期区块的极高收益回报，并引导合理使用可再生资源。

一些加密货币已经选择在某些时候引入固定常数的收益（例如狗狗币dogecoin）。这将意味着现有货币最终的一个线性通货膨胀和货币贬值，所以我们避免这种

做法。其它货币已经引入了一些与外部效应诸如哈希率成比例的收益（例如点点币peercoin）。我们也拒绝这种做法，因为它在货币供应量的计算上有不确定性，以及未来线性通货膨胀的潜在可能。这些方法试图通过确保对挖掘硬币的兴趣来增加货币寿命，但是要有成本。通过木币的方法，我们确保了伐木激励的长寿命，但没有无限制或不确定的通货膨胀的负面影响。

绘制总货币量相对区块数的木币平滑释放曲线也许是最好的说明，我们将会在图1和图2中表示。

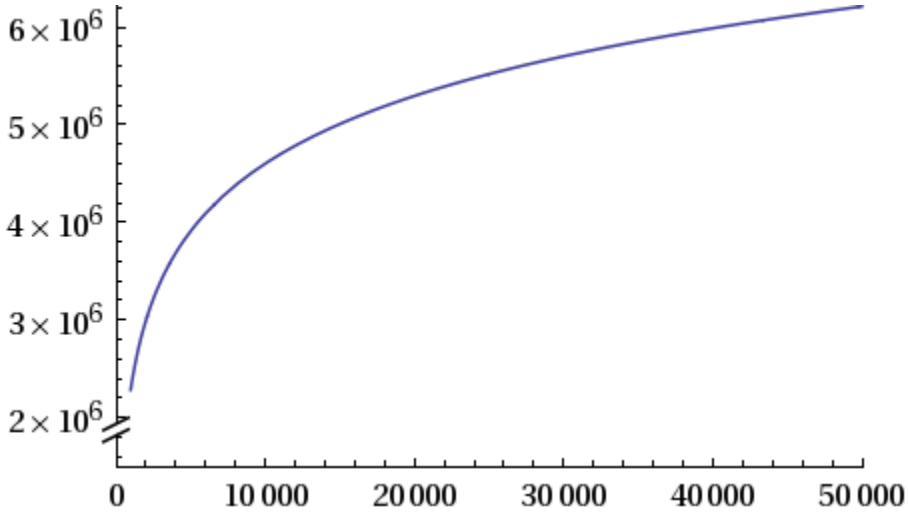

图1.从0到50000个区块对应的木币总供应量

通过比较图1和图2可以看出，对数函数的一个重要特征是自相似性。在任何一个区块，虽然收益持续下降，但伐木者当下的得利依然会比任何将来的伐木者要多。当前砍伐木材的动力依然存在，而且不会人为减少。

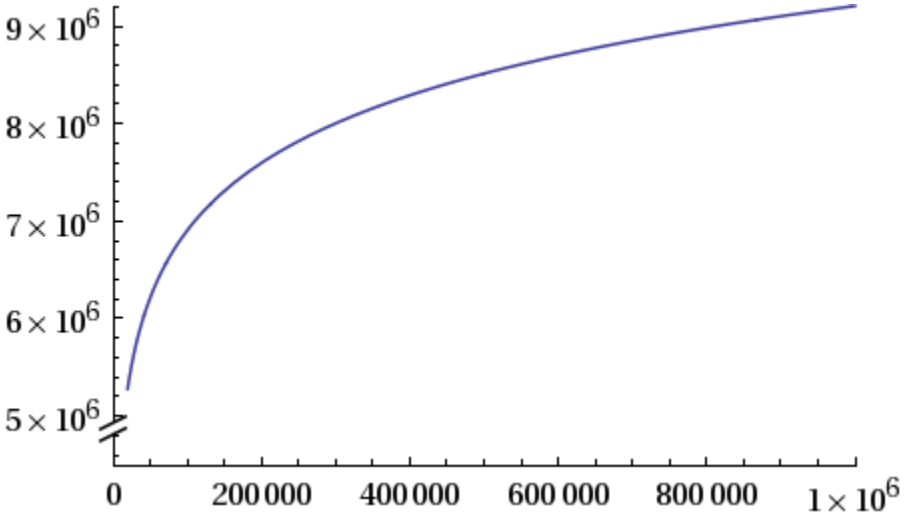

图2. 从0至100万个区块对应的木币总供应量

工作算法证明

在选择哈希函数为工作和形成区块的验证交易提供证明时，在加密货币的世

界中存在很多差异。许多货币选择函数，试图允许普通CPU挖掘，而不给予用专用硬件的激励。如果这些货币成功地获得了价值，他们的这一努力将失败，因为所有的算法可以在正确的硬件上更快地执行。我们选择哈希函数，并不是试图避免ASIC或者GPU伐木，而是因为我们发现它在实现中是最安全的和最能理解的，所以选哈希函数。Skein函数的描述和推广最好留给其创造者[Ferguson等人，2008]，因为这超出了本文的范围。但是我们在这儿指出两个关于Skein哈希函数的事实：

1）布鲁斯·施奈尔（Bruce Schneier）创建了其中一部分。

2）国家安全局（NSA）没有选择将其作为官方的SHA3哈希函数。

椭圆曲线数字签名算法（ECDSA）的椭圆曲线选择

也许使加密货币成为可能的最重要的技术是数字签名算法，它让参与者证明货币的所有权，进而花费它。这项技术于1976年被伟大奇才威特菲尔德·迪菲（Whitfield Diffie）和马丁·海尔曼（Martin Hellman）首次推广。 对历史的适当讨论超出了本文的范围，但应该指出的是，他们1976年的文章已经预测了数字交换商品的兴起。像大多数加密货币一样，我们选择使用与该文章中介绍的算法所不同的算法来形成数字签名：我们使用椭圆曲线数字签名算法（ECDSA）。使用该系统需要选择特定的椭圆曲线。选择曲线后，可以通过选择该曲线上的点来选择专用密钥。虽然我们知道任何流行的曲线选择没有实际的弱点，但是我们会借此机会进一步的介绍加密的多样性，并选择与大多数其他加密货币不同的曲线，使用了一种称为secp256k1的曲线。我们使用的曲线被称为ANSI X9.62 Prime 256v1，是在世纪之交被公布为金融机构推荐的曲线[ANSI，1999]。

结论

在阅读上述关于木币属性的技术讨论时，一个重要的元素已经被忽略了。那就是我们看到了树却错过了森林。伐木注定是一种有趣的处理加密货币的新方法，并鼓励我们暂时离开矿井，惊叹于树木的美丽。伐木是令人振奋的，在我们伐木的时候，由于我们细心的可持续发展规划，我们可以认为这个资源将会一直持续到未来。我们还记得维护森林和多样化生态系统的重要性，并且考虑和尊重树木的智慧和新鲜的凉爽空气的礼物。 随着加密货币的向前发展，不可再生能源的进一步枯竭，预计双重使用伐木和家庭取暖将变得更加普遍。木材也是其它技能的重要资源，我们希望一旦实现了原子交叉链交易，就可以发展LOG以用于其它各种各样的加密货币应用。

“区块链是伐木结构化数据库”- Funkenstein the Dwarf

参考文献：

1） “Bitcoin: A peer to peer electronic currency”, Satoshi Nakamoto, Oct. 31, 2008

2） “The Skein Hash Function Family”, Niels Furguson, Stefan Lucks, Bruce

Schneier, Doug Whiting, Mihir Bellare, Tadayoshi Kohno, Jon Callas, Jesse Walker, Nov. 15, 2008

3） ANSI X9.62, “Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)”, 1999