PPC:
一种P2P（点对点）的权益证明(Proof of Stake)密码学货币（修订版）

Sunny King, Scott Nadal
(sunnyking9999@gmail.com, scott.nadal@gmail.com)

8月 19日, 2012年
翻译：gzlitao@gmail.com

摘要：
PPC是从中本聪所创造的BTC衍生出来的一种P2P的电子密码货币，以权益证明（Proof of Stake，以下简称PoS）取代工作量证明（Proof of Work，以下简称PoW）来维护网络安全。在这种混合设计中，PoW主要在最初的采矿阶段起作用。长远来看，PPC网络的安全并不依赖能源的消耗。因此PPC是一种节能而有成本优势的P2P电子密码货币。PoS是基于币龄(coin age)并由通过与 BTC类似的由每个节点散列运算产生的，只是其搜索空间被限制了。区块链的历史及交易结算是通过一个中心化广播检查机制得到进一步保护。

背景

自从中本聪在2008年创造出比特币以来，工作量证明(PoW)的设计理念已成为P2P电子货币的主流思想。在中本聪的设计中，PoW是保证采矿及BTC安全的支柱。

在2011年10月，我们意识到币龄（coin age）可以是中本聪PoW设计以外的另一种设计，即权益证明（PoS）的基础。自从那时起，我们就开始构思利用PoS来构建P2P现金的安全模式及一部分造币流程，而PoW主要在最初的造币阶段起作用，而重要性逐渐减少。此设计试图展示将来可在不依赖消耗能源的情况下，P2P密码学货币仍然是可行的。我们将此项目命名为PPcoin.

币龄(Coin age)

至少早在 2010年，中本聪就在BTC设计中提出并使用了币龄这一概念，用于给交易排出优先次序，但这个概念在其安全模式中没有起来很重要的作用。币龄只是简单地定义为货币的持有时间段。简单举例说明一下：如果李明从韩梅那里收到了10个币，并且持有90天，那么李明就收集到了900币天的币龄。

此外，如果李明使用了从韩梅收到的这10个币，我们就认为李明从这10个币上积累的币龄被消耗（销毁）了。为简化币龄的计算，我们为每个交易引入了时间戳的概念。区块时间戳及交易时间戳相关联的协议得以强化，以便确定对币龄的运算。

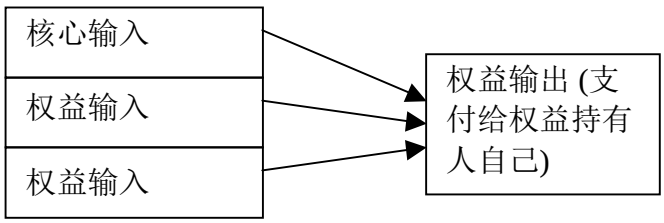
PoS权益证明

PoW是中本聪在技术上的主要突破，但PoW的本质意味着BTC需要消耗能源来维护运行，维护这样一个网络的运转需要消耗大量的成本。这是用户通过通货膨胀及交易费的组合来支撑的。随着BTC网络采矿产出下降，最终其可能提高交易费用来维持整个网络的安全性。很自然地我们就会问：是否一个去中心化的电子货币，都必须消耗大量能源（来维持运行）呢？因此PPC在理论上和技术上都是一个非常重要的突破，即P2P的电子货币系统并非一定要依赖能源消耗才能维持其安全。

早在2011年BTC圈子中就有了对PoS权益证明这个概念的讨论。大概说来，PoS指的是一种对货币所有权的证明。一笔交易所消耗的币龄可被视为PoS的一种形式。我们在2011年10月独立发现了PoS及币龄的概念，当时我们意识到通过对BTC造币及安全模式精心地进行重新设计，PoS实际上可以取代POW的大部分功能。这主要是因为，和工作量证明PoW一样，PoS权益证明也不可能被轻易伪造。当然，这也是货币系统中的一个关键特性-防止伪造。从哲学角度而言，货币在过去就是一种“工作量证明”，因此其本身可以代替工作量的证明。

PoS设计下的区块生成

在我们的混合设计中，区块被分成两种形式，PoW区块及PoS区块。



图三：PoS交易（利息币）的结构

在这种新型区块里PoS是一种特殊的交易称利息币(coinstake)（依据BTC当中的一类特殊交易：币基(coinbase)而命名）。在利息币(coinstake) 交易中，区块持有人可以消耗他的币龄获得利息，同时获得为网络产生一个区块和用PoS造币的优先权。利息币的第一个输入被称为 核心（Kernel），并需要符合某一Hash目标协议。由此PoS区块的产生具有随机性，这一过程与PoW相似。但有一个重要的区别在于，（PoS）随机散列运算是在一个有限制的空间里完成的（具体来说为1 hash/未消费钱包的输出*秒），而不是象PoW那样在无限制的空间里寻找，因此无需大量的能源消耗。

权益核心(kernel)所要符合的随机散列目标是以在核心中消耗的币龄的目标值（币*天coin-day）（这与BTC的PoW是不同的，BTC的每个节点都是相同的目标值）。因此核心消耗的币龄越多，就越容易符合目标协议。例如，如果李明的钱包里放了100个PPC，而且1年都没有动，那么他可望在2天内产生一个权益核心（个人理解为PoS的区块）；同理，如果韩梅有200个PPC，也放了1年没有使用，那么她可能在1天内就能产生一个权益核心。

在我们的PoS及PoW设计中，随机散列的目标值都是持续调整的（难度的调整）。这与BTC约每两周一次调整不同。主要目的是为避免采矿产出的突然波动。

基于PoS的挖矿（minting）

除了BTC的PoW区块之外，在PPC中还有一种新型的PoS造币过程。PoS区块将根据在币利交易中所消耗的币龄产生利息币。设计时设定了每1币一年将产生1分（利息），以避免将来的通胀。

虽然我们在造币时保留了PoW，使最初的造币更加方便，但是可以预料到的是在一个纯粹的PoS系统里，最初的造币可以种植在创世区块里，形式类似于现实证券市场中的IPO。

主链协议

判断主链的标准已经转化为对消耗币龄的判断。每个区块的交易都会将其消耗的币龄提交给该区块，以增加该区块的得分。获得最高消耗币龄的区块将被选中为主链。

这与BTC主链协议中以PoW工作量最高的为主链的协议是不同的。

此设计减轻了部分对于51%攻击的忧虑，因为在 BTC网络中，诚实的节点至少需要占据51%的算力才能维护网络的安全。（而在PoS区块中，要进行51%攻击）首先要控制数量众多的PPC，成本可能要高于获得51%的算力，这样就提高了攻击的成本（攻击者需要控制51%以上的PPC）。其次，攻击者在攻击网络时，其币龄也会消耗，这将使得攻击者阻止交易进入主链的行为变得更加困难。（类似算力增加不单是增加分子，也增加在分母上。）

校验机制:保护历史数据：

使用消耗币龄总数来决定主链的不足之处在于其降低了攻击整个区块链历史的成本。即使BTC在保护历史数据方面有较强的机制，但中本聪仍在2010年提出了校验机制来保护区块链历史，防止任何可能在校验点之前对区块链的修改。

另外一个忧虑是双重支付的成本也可能降低了，由于攻击者可以累积一定量的币龄来迫使区块链重组。为使此系统在商业上具操作性，我们引入了一个中心校验机制，每一天大概会向全网广播若干次，以冻结区块链及结算交易。这种新型的校验机制与BTC的警报系统类似。

Laurie(2011) 提出BTC并没有完全解决大家的担忧，即校验机制没有发布给大家。我们尝试设计一种可行的去中心化的校验机制，但发现在对抗网络分叉(fork)时很困难。虽然向全网广播的校验机制是一种中心化的形式，但在没有去中心化的解决方案之前，我们认为这是可以接受的。

另外一个使用中心化的广播校验机制的原因是：为了抵御一类DOS攻击，在每个节点都接纳一个PoS区块到本地数据库（区块树）之前，权益核心必须得到验证。由于BTC的节点数据模式（交易索引），需要为数据校验设定一个最后期限，以确保在采纳PoS区块进入区块权之前，所有节点都有能力校验与每个权益核心的联接。从实用角度考虑，我们决定不修改节点的数据模式而是使用中央校验机制。我们的解决方案是修改币龄的计算，设置一个最低币龄，比如说一个月，低于这个数字将计算为零。然后中央检验机制被用于确保所有节点都认可过去所有大于1个月的交易，由于核心要求不低于零的币龄，这样就让允许权益核心得以验证，这样就必须使用大于一个月的输出。

区块签名及双重权益协议

每个区块都必须由其拥有者签名，以避免同一PoS受到复制并被攻击者使用。

为了抵御攻击者使用单个PoS来产生多个区块进行DOS攻击，我们在设计上采用了双重权益协议。每个节点都会收集其接触到的（核心，时间戳）配对的所有利息币交易信息。假如一个已接收到的区块包含与其它之前收到的区块中的配对信息（核心，时间戳）是重复的，我们会忽略此区块直到后者被孤立(orphaned)出去。

节能

当PoW采矿产出趋近于零时，其对矿工的激励作用就会越来越弱。长远来看，由于矿工失去使用PoW方式采矿的兴趣，网络消耗的能量就会降到非常低的水平。除非交易量/交易费用升到相当高的水平，否则 BTC网络将难以维持这样能源消耗。在我们的设计中，即使PPC网络中消耗的能源接近于零，其仍被PoS保护着。假如一种电子密码货币允许PoW趋于零的话，我们将这种币称为长期节能货币。

其它考虑

我们把PoW的采矿产出率修改为随难度变化，而不是随着区块高度（时间）而调整。当采矿难度升高，PoW采矿产出率下降。与BTC的分步减半产出相比，PPC的产出曲线相对平滑，以避免人为地动摇市场。更具体地说，每当难度升高16倍，采矿产出就会减半。

在摩尔定律下，长期而言，PoW的产出率不会与BTC的通化膨胀行为有大的区别。根据传统看法，我们认为更明智的做法是市场更青睐低通胀货币，而非高通胀货币，尽管出于理想主义的原因，某些主流经济学家对BTC进行了严厉批判。

Babaioff et al.（2011）在研究了交易费用的效果后，认为交易费用将鼓励矿工们互相不合作。在我们的设计里，这种攻击加重了。所以我们不再给发现区块的矿工奖励交易费。我们决定销毁交易费用。这样就去除了矿工们互相不承认对方区块的动机。这也成为平衡PoS造币所产生通胀的通缩措施。

我们也在协议层面执行交易费，以防止区块膨胀攻击。

在我们的研究中，除了PoW及PoS外，我们还发现了第三种证明系统，PoE（Proof of Excellence，试译为优秀证明）。在这种系统里，可以定期举办某种采矿比赛，根据参与者的表现来派发采矿收入，模拟在现实生活中的比赛的不同奖励。虽然这种系统在人工智能在参与的比赛中占优时，也倾向于耗费能源，但我们仍然觉得这种概念非常有趣，因为这种机制提供了某种更灵巧的消耗能源的方式。

结论：

在市场上验证我们的设计时，我们希望PoS成为一种比PoW更加有竞争力的密码学货币，由于其消除了对能源消耗的依赖，从而在可比较的网络安全水平下，达到了低通胀/低交易费用的结果。

鸣谢：

感谢Richard Smith提供的测试及各种网络/分叉相关的工作。

感谢中本聪及BTC团队做出的杰出贡献，没有他们，本项目也就不可能实现。

参考文献：

Babaioff M. et al.(2011):On Bitcoin and red balloons.

Laurie B.(2011):Decentralised currencies are probably imPoSsible (but let’s at least make them efficient). (http://www.links.org/files/decentralised-currencies.pdf)

Nakamoto S.(2008):Bitcoin:A peer-to-peer electronic cash system. (http://www.bitcoin.org/bitcoin.pdf)