比特股 X

去中心化的银行和交易所

作者：**Daniel Larimer**

dlarimer@invictus-innovations.com

2014 年 2 月 14 日

翻译：试手补天 yidaidaxia http://weibo.com/u/1776463184

log☆logxing http://weibo.com/u/1092405564

校对：暴走恭亲王 http://weibo.com/u/1402559840

巨蟹 http://weibo.com/u/2792936064

摘要

比特币等加密货币开启了信息时代的经济革命大门，其重要意义不亚于此前的工业革命。比特股 X 将比特币所引入的想法带到了一个新的水平，是第一个使用非信任机制数字资产并使该数字资产可能跟踪任何事物价格的实验。在本白皮书中，我们将分享比特股 X 设计和功能的详细信息。

1.0 背景

2013 年 5 月 24 日，Daniel Larimer 在 bitcointalk.org 的一个帖子里首先提出了相关想法，而比特股 X 则是这些想法的第一次实践。这些想法发展和完善了一段时间，然后被总结为发表在 letstalkbitcoin.com 上名为“对于安全性的过度支付”的文章中所引入的新概念，

即加密货币应该被视为股权，从而着眼于用最低成本产生最大价值的方式最大化利润。这也就是现在已逐渐为大家所知道的所谓“分布式自治公司”(Decentralized Autonomous Company，简称 DAC)。

比特币可以被看作是一个 DAC，其中交易费就是收益，矿工是员工。在比特币的例子中，运营费用超过运营所得，因此比特币正以一种亏本的方式进行运营，(在写这篇文章的时候)每年大约损失 10 亿美元。比特币的商业模式以硬编码的形式写入块链，并且 100 年内都不会达到收支平衡。

一个 DAC 的目标是通过增加由交易提供的价值而最大化来自于交易费的收益，同时最小化运营成本。DAC 不创造货币，而是由股权构成，更像是公司。一份股权就是所占整体份额的一个百分比。有很多方法来分配股权，先前的做法是将其分配给员工以依靠算力保障网络安全。然而，对新员工发行股权会使老员工所持股权的价值贬值，且传统商业概念会将其理解为一种花费。

1.1 安全性

对于如何保障网络安全有三种想法，工作量证明机制、股权证明机制以及投票共识机制。安全性的目标是使更改交易历史或产生伪造区块的行为在经济上不可行。这很重要，因为如果没有防止伪造行为的能力，那么没有人可以确信他们认为自己所拥有的股权将来是否会被其他人承认。此外，网络也必须保证能抵抗拒绝服务攻击，防止有人有能力通过网络阻止所有的或部分的交易进行。

1.1.1 工作量证明机制 (Proof of Work，简称 PoW)

工作量证明概念最初由 Adam Bach 作为一个防止垃圾邮件的方法提出。这一概念是指算出某些特定计算的解比较困难但验证其正确性则比较容易。使用工作量证明机制，一个攻击者为制造数据所需消耗的资源将远远超过任何其他人为验证这些数据所花费的资源。

比特币用工作量证明实现了一些目标。制造一个区块所花费的时间与财富成本变得越来越昂贵，因而越来越难以伪造。同时，该机制也意味着平均来说某一时间只会有一台电脑找到一个区块。从而自然地解决了由谁来制造下一个区块的问题。

理论上来说，这种分布式区块生产使得单个不良行为者所要进行的工作比其他所有诚实者一起做的工作还多，从而使这种行为在经济上无效率。该理论在比特币的开始阶段很有效因为没人对其进行严肃研究，但经过进一步仔细检查，我们发现该安全模型有其根本缺陷。

完成工作量证明是为了赚取利润，因此对于这些每一点点奖励可以完成最多工作的人将会赚取最多的利润，而将效率较低的竞争者挤出局。这意味着规模经济将导致工作量证明的中心化。在比特币的例子里，挖矿已经被中心化，由五六个矿池掌控，并且将被大的私人 ASIC(Application Specific Integrated Circuit，特定用途集成电路)矿机开发者变得更中心化。现在，某一两个玩家已经有可能阻止交易加入网络，而将来，政府可能由此实现强迫冻结特定转户的余额。

所以，工作量证明机制在付出巨大的成本的同时，还产生着它本想防止的特定情况：中心化，从而最终侵蚀着一个 DAC 的价值前提。由于这个原因，工作量证明机制不是一个保障交易总账安全的适当模型。

1.1.2 股权证明机制 (Proof of Shake，简称 PoS)

股权证明的概念最初被当作一个对抗对于工作量证明机制网络的攻击的方法而引入，尤其针对 51%攻击。51%攻击将使得攻击者可以进行拒绝服务和交易筛选以及双重支付。

现有的股权证明系统，例如点点币(Peercoins)，是构建在“证明区块”上的，其中矿工必须满足的目标与币销天(coin-days-destroyed，简称 CDD)负相关。拥有点点币的人必须选择成为一个股权证明矿工，并且承诺锁定一部分他们的币一段时间来保障网络安全。

点点币的创造者认识到这种形式的股权证明是不足以保障安全性的，所以他们依靠一个股权证明和工作量证明的混合系统来保障网络安全。

一个最近的股权证明类型的加入者是 NXT(NextCoin，未来币)，它宣称 100%使用股权证明，并通过他们称之为透明挖矿的方式将其实现。通过透明挖矿，网络可以确定地选择谁制造下一个区块。如果此时这个人在线，那么他们将有机会赚取交易费。否则这个区块将由系统选择的下一个人制造。

包括点点币和 NXT 在内的现有股权证明系统的问题是，它们依赖于用户群的一个子集，这部分人实际上选择将其算力投入挖矿来从交易费中获得收益。这将用户分成了两种，并极大的减少了提供保障网络安全的财富所占的百分比。另外，这两个系统都可能遭受一个大量股权持有者通过拒绝加入部分或所有交易来进行的拒绝服务攻击。

1.1.3 共识机制 (Consensus)

共识机制首先由瑞波币(Ripple)引入。瑞波币有一个非常重要而又基本的认识，那就是在一个市场里要想使每个人都达成一致的充分必要条件是就每个人的最佳利益达成一致。然后他们将该认识与这样的事实结合，那就是如果有足够多的带有不同利益并互相竞争的节点，则他们几乎不可能合谋欺骗你，而当他们在网络里拥有公共信誉的情况下则更是如此。

与其他体系一样，瑞波体系建立了一个交易总账以及签署该总账的不同节点。通过使用一套偏向于彼此达成一致的投票系统，节点间能够就以什么样的顺序将新交易加入达成一致。这些节点不需要防范伪造交易记录，因为他们总是保持同步，而当其重新连接进网络的时候，只要简单地相信多数方就可以了。

这个体系并非没有成本。为达成共识，节点间必须交换额外的信息。瑞波节点不通过交易费获取报酬，而是在流通循环中将交易费相对应的 XRP(瑞波货币)进行销毁。将交易费进行销毁的行为等同于支付红利。就像这样，瑞波网络是第一个产生利润的 DAC。

1.1.4 基于交易的股权证明机制（Transactions as Proof of Stake，以下简称 TaPoS）

2013 年 11 月 28 日，Daniel Larmier 发表了一篇关于新型股权证明机制的白皮书，该

机制利用了这一事实，即网络中每个进行交易的人，都在当前网络状态中拥有利益。

基于交易的股权证明机制按这一原则运行，即 DAC 的股东应该决定并批准交易总账。每个股东因其持有股票而对每个区块有每股一票的投票权。当交易发生时，通过对前一区块的 hash 值进行签名，股东对当前的交易总账状态同时进行投票。当该交易含有股东预期之外的台帐时，计票结果将有助于保障网络安全。一笔投票赞成一个无效台帐的交易，其相关投票数将是无效的。

每个单独的区块，在被加入总账之前，都必须满足一个最小投票数。这保证了没人可以在前一区块没得到充分批准前生产一个新区块，并且该最小投票数主动地、持续不断地在网络得到里增加。随着交易总账越来越大，积累的投票越来越多，历史交易总账变得不可改变，于是安全性得以保证。

股权证明机制解决了安全问题，但是没有解决关于下一个区块应该是什么内容的共识。这一共识可以通过很多方式获得。其中之一是使用瑞波形式的共识算法，另一个方式是使用工作量证明形式的彩票系统。两个系统都可以使用，也各有其优缺点。

如果选择工作量证明形式的彩票系统，那么在获得足够多的投票之前，制造下一区块的难度将为无穷大，而获得足够多的投票之后，系统使用标准的比特币形式的难度调整来进行挖矿以产生下一个区块。与比特币不同，该系统的安全性不靠挖矿提供，那些排除交易区块的矿工也排除了产生区块所需的投票。由于每个人必须纳入尽可能多的交易来积累开始挖矿所必需的投票数，该特性使得拒绝服务攻击变得不可能进行。

对于那些没有从交易获取足够投票数的区块，自己拥有一些股权的节点可以选择使用一些他们自己的投票来开始挖矿而生产该区块，通过这样的方式，这些节点可以比其他节点多一些优势。一个矿工使用自己的投票的动机是他们因此可以赚取交易费。在某种意义上，节点通过投票有规律的获得回报，从而给网络安全提供了确定的保障。

与你有多少 hash 算力无关，某个人不可能通过垄断新区块的产生而将第三方交易长时间排除在外。他们将不得不消耗他们自己的投票，而一旦他们的投票被用完，其他人就将把被他们排除在外的交易纳入新区块。

比特股 X

2.0.0 比特股 X 介绍

BisShares X 是一项测试一种新型“可预测市场(Prediction Market)”背后的经济理论的实验。该实验创建了去中心化的银行和交易所，使用由 ToPoS 保障安全的去中心化交易总账来创造可互换数字资产,这些资产可以市场化锚定美元、黄金、汽油等任何东西的价值。和所有的 DAC 一样，比特股 X 拥有可以像比特币那样在用户间转让的股权。比特股 X 的特殊之处是它实施了一个类似于银行或经纪公司的商业模式。在本白皮书里，我们把比特股 X 的股权称为 XTS，并用锚定美元的比特美元(BitUSD)来作为比特资产(BitAsset)的例子。

比特股 X 可以通过抵押贷款的方式创建比特美元，正如今天的银行系统提供美元贷款一样。银行用你的房子作为抵押品，而比特股 X 用 XTS 作为抵押品。如果抵押品的价格相对于比特美元下跌，那么比特股 X 将自动卖出被抵押的 XTS 来偿还欠款，并将剩余的 XTS 返还给比特美元借入者。

借入比特美元的目的是为了相对于 XTS 卖空比特美元。这与做空一支股票的方式一样。首先，你借入股票，然后以今天的(较高的)价格将其卖出。如果一切顺利，那么你明天就能以比你今天卖出价低的价格将其买回，偿还你的借贷，得到收益。然而，如果事情的发展和你想要的相反，那么你将不得不用比你卖出所得更多的钱将股票买回，并承担损失。

比特美元产生于两个对手方就某个价格达成的一致，而双方能达成一致的唯一价格将是目前美元与 XTS 的市场兑换价格，否则其中一方将开始亏损。市场锚定机制和“可预测市场”机制十分类似。一旦市场就比特美元应与美元价格相同这点达成共识，那么任何人进行违反该共识的交易都将损失财富。这样，今天比特美元的价格将基于市场参与者对比特美元未来价格的预测。只有一种理性推测方式，那就是共识将会持续有效，从而创造出了一个自我加强的市场锚定机制。

在比特股 X 里，所有的空头头寸(借入比特美元)必须用足够多的 XTS 来创建，因为借入比特美元需要双倍抵押 XTS。当抵押品(XTS)的价值下跌到借入物(比特美元)的 1.5 倍时，保证金(抵押品、XTS)将会被系统收回。这使市场在抵押品不足前有大量的机会来对空头进行补仓并兑付借款。在市场执行强制平仓的情况下，网络将额外收取 5%交易费用。这将激

励市场参与者积极主动地管理他们的保证金。

在极端情况下，如果 XTS 的价值在一小时内快速下跌 50%而导致抵押品不足，100%的抵押品将被用于尽可能多的偿还比特美元空头仓位，并仍将有一些比特美元空头寸无法平仓。这一价格波动的结果将导致某些流通中的比特美元没有抵押品支持，这可能影响、也可能不影响比特美元对美元的市场锚定机制。对于市场对此情况的反应，我们有两种假设：一种假设是比特美元将开始以折扣价交易，折扣比例取决于流通循环中所多余的这部分比特美元的占比。另一种假设是，市场对于锚定机制的预期将压倒任何(比特美元)过量供应，从而比特美元将像原先那样交易。这与美元脱离金本位后没有立即价值归零的情况十分类似。

3.0.0 实现细节

为了实现比特股X，我们利用了一个类似比特币的块链结构。对于比特币来说，每一笔交易采用上一笔交易作为输入，并且生成一个可以在将来的交易中用作输入的输出。每一个输出仅可使用一次，使用时要满足一定的条件。每一个输出包含一个比特币余额，该余额可以添加到将来的交易中。一个交易所有输入的总值必须大于输出的值，以维持这样一个属性：任何交易都不能凭空创造比特币。

比特币使用一个简单的脚本语言来评估可以花费哪一个交易输出的余额；然而，所有交易输出的绝大多数只是要求其所有者的加密签名。

3.1.0 交易类型

比特股X认识到，当所有的交易使用相同的脚本时，脚本语言的灵活性是根本不必要的开销。在比特币的情况下，脚本能做的事情有限，因此我们无法使用比特币脚本建立比特股X。取而代之，我们定义了一组固定的七个声明条件：

3.1.1 签名声明

允许花费输出，前提是提供了所有者签名。这就像一个标准的比特币输出脚本。

3.1.2 N of M签名声明

允许花费输出，前提是提供了M个所有者中N个所有者的签名。这就像一个比特币多重签名输出。

3.1.3 买单声明

允许花费输出，前提是指定的资产类型以指定的价格支付给了买单的拥有者。一个买单可以部分成交，只要一个包含了变化的新的买单同时被创建了。买单仅能以确定的方式，在根据市场匹配算法创建了一个新块时，与其他的*买单声明，多头声明或平仓声明*输出相匹配。一个买单声明输出也可以通过拥有者提供一个签名来花费掉，通过这种方式拥有者可以取消他们的下单。

3.1.4 多头声明

允许声明输出，前提是拥有者以指定的价格创建了*空头头寸*（平仓声明）。空头头寸必须与一个新的，创建了等量的新比特美元的*签名声明*输出配对。这个输出也可以通过拥有者提供一个签名来花费掉，通过这种方式拥有者可以取消他们的下单。

3.1.5 平仓声明

允许抵押品支持一个空头头寸以被同一个交易销毁的比特美元量的比例为依据被访问。

比特美元通过包含它作为一个没有相应输出的输入来被销毁。该输出仅能被它的拥有者平仓，除非在订单匹配算法的确定性操作中，它被用作追加保证金的一部分。

3.1.6 行使期权声明

允许取得优先买卖权的人在给定的日期前花费输出，前提是他们对优先购产授权者支付了指定的款项。在指定的日期之后，输出仅能被优先购产授权者声明。

3.1.7 密码声明

用于跨链交易，允许一个输出以以下两种情况之一被花费：提供两个签名，或一个签名和一个密码。

3.2.0 交易费用

比特股X 试图通过最小化入门壁垒来确保去中心化。带宽和磁盘空间是两个必须保持足够低的入门门槛，平均而言个人应能作为一个完整的网络节点参与。为了实现这一点，我们已经选定了区块最大大小为1MB每5分钟以及最大区块寿命为每个输出一 年。这意味着每个节点仅需要储存至多大约100GB数据每年(不包括索引)。然而，虽然最大区块大小为1MB，区块大小的目标值为512KB，交易费用会以保持区块大小小于512KB为目标自动调整。交易费设置为每字节的价格，以XTS支付。

调整交易费的算法如下：

next_fee_base = block_size * previous_fee / (512*1024);

next_fee = (99*previous_fee + next_fee_base) / 100;

next_fee = max(next_fee,min_fee);

这个算法会在大于512KB的区块产生时提升价格，在小于512KB的区块产生时使价格跌向最小费用。价格上涨将会减少交易需求而下跌将会增加需求。因此块链有一个设置价格的自动机制。这应该可以减少为了要将一个交易包含至块中一个人要付多少手续费（就像比特币用户所经历的那样）这个问题的复杂性和不确定性。

最低交易费用是这样设置的：如果所有的区块都是512KB，那么每年0.5%的股权供应将作为交易费。

3.3.0 红利

因为我们视比特股X 为一个旨在获取利润的DAC，所以它应该对持股者支付红利。红利从被销毁的交易费中支付。减少XTS的供应在经济上等同于对XTS的所有持有者按其持有比例分发交易费。

虽然很多用户可能不喜欢通过销毁股权的方式获取正回报，而是更喜欢一个增长的帐户余额，这个细节可以在用户界面中被修正而不是在块链本身上。比特股X 会以当前股权供应的百分比显示一个用户XTS帐户余额，如此用户就可以看到他们的余额在每一个块都在增长。

当用户花费他们的XTS时，用户界面将根据比例转回实际的股权来生成一个块链上的交易。

3.4.0 区块生成

区块的生成是用TaPoS算法和比特股PTS首次引进的Momentum工作量证明共同完成的。挖矿的难度根据过去24小时的平均块间隔和以每5分钟一个区块为目标进行调整。没有挖矿奖励，交易费按与第三方交易相关的矿工提供的股权证明投票数量的比例分配。不做任

何股权证明投票的矿工不会获得任何交易费。只提供1%投票的矿工获取1%的交易费。

每一个区块上的时间戳必须大于它的前一个区块并小于当前时间，否则就不能通过网络传播。

如果两个区块同时产生，则拥有更多投票的区块胜出。在“抢七”（网球术语）中失败的矿工的投票将会自动计入下一个区块。

4.0.0 订单匹配算法

比特股X运用非传统的订单匹配算法。这种算法选择能恰好满足买方的需求，而不是像传统订单匹配那样至少满足买家的需求，有时会多一点。在任何时候，当最高价买单大于最低价卖单时，其差额会被网络识别计为手续费。

选择这种算法的理由是为了惩罚那些企图以大单交易产生吃价过深的手段通过按一次性账面量比例获利的方式来操控市场的人。这样做的目的是强制执行价值投资而非技术交易。没有市场参与者会因为得到了他们自己想要的东西而抱怨，他们只会下他们认为公平的订单。

这种计费系统导致的结果是一些比特美元无法参与流通并被有效地销毁。 当流通中的比特美元少于空头需要平仓所需的量，这对比特美元的价格支持提供了不断增长的基础。从许多方面来讲，这就像是你的比特美元赚取了红利或利息。

首先，所有的买单和卖单相匹配，然后，如果最高价买单高于任何*平仓声明*仓位的追加保证金临界值，抵押品会从有最少抵押品的仓位开始用于接受买单。

5.0.0 设想

比特股X是一项经济实验，我们相信市场可以自动地对数字资产的存在达成共识，认同在抵押品的支持下，数字资产可以与任意现实世界的资产保持高度的关联性，从而创建一种

具备美元的价格稳定性并具有比特币的所有其他属性的数字货币。这就是说，还没有一种有比特股X独特特性的系统被创建起来。下面我们将介绍一些我们的设想，但并不承诺比特美元会以任何特定的方式运作。

5.1.0 1 比特美元将可以始终窄幅追踪 美元 / XTS 汇率。

这一设想是基于认为预测市场需求的基本面将可以解决任何比特美元空头仓位的数量和流通中比特美元的数量不匹配的问题。

5.2.0 1 比特美元将高度相关地追踪 美元 / XTS 汇率，但有一个相对固定的溢价或折价，溢价或折价在极端的市场活动中可能会偶尔改变。

这一设想基于的事实是，流通中的比特美元会比空头平仓所需的量或者多或者少，这样的不匹配会导致一定比例的溢价或折价。这也是基于这一事实：比特美元稳定的销毁成市场交易费可以被视为正收益。另一方面，XTS价格快速下跌所导致的抵押下的比特美元的风险会导致比特美元相对美元有一个轻微的折价。只要和美元/XTS的价格变动有高度关联性，是否会溢价或折价最终都无关紧要。

译注

为避免概念混淆，特请读者注意：本白皮书（比特股 X 白皮书，或称为新版比特股白皮书）中的比特股 X(BitShares X)，其概念对应于比特股白皮书(老版比特股白皮书)中的比特股(BitShares)，而比特股(BitShares)这个名词本身，则“升级”为 Invictus 公司 DAC 产品的总品牌。亦即，比特股 X 作为去中心化的交易所和银行是未来将推出的诸多不同类型的比特股 DAC 中的一个，后续计划还将推出各种不同类型的，例如 BitShares DNS，BitShares Bingo，BitShares Music，BitShares Vote，又或者已经推出的 PTS，AGS 可以被称为 BitShares PTS，BitShares AGS，等等。

比特股 X

译者后记

- 比特股 X 白皮书的翻译工作从比特股白皮书的译文中获益匪浅，并力图做到两个白皮书之间的中文概念与用词习惯保持一致。在此特别感谢比特股白皮书的译者巨蟹和暴走恭亲王百忙之中抽出时间进行校对与指正。此外，KingZhang(http://weibo.com/kimjzhang)与_云晨(http://weibo.com/u/1863583752)对本译文亦有贡献。

- 本白皮书的英文原版本身如作者所言将随着产品开发进行更新，更多最新信息还请关注比特股官方论坛 bitshares.org。同时，也十分欢迎您对译文内容提出宝贵的意见或就相关内容进行探讨。