

## 第20讲 | 区块链项目详解：比特股BTS

2018-05-09 陈浩

深入浅出区块链

[进入课程 >](#)



讲述：黄洲君

时长 10:42 大小 3.70M



前面两篇我们都聊了智能合约的话题，智能合约可以说是当下区块链最热的概念了，在多数人眼里，没有智能合约的区块链价值几乎就大打折扣。

那么说，实际上是不是这样呢，我们今天就来聊聊一个并没有开放式智能合约的区块链项目——比特股。

比特股发布于 2014 年，虽然没有引入智能合约的概念，但它提供了功能极为丰富的金融类工具，比特股上所有的金融合约都是事先在代码里写好的，所以说它的本身就是一个超级智能合约集合。

### 什么是比特股

比特股是一个公开透明的、7\*24 小时不间断运行的、基于区块链技术的去中心化交易平台。

□它兼具了区块链的优点，也是第一个有关稳定数字货币的尝试，目前比特股提供了若干核心的金融服务，例如支付、撮合交易、资产存托等服务。

□相较于传统的金融 IT 系统，它的服务器是由分散在世界各地的受托人（Delegated）维护的，即使其中一些人被攻击也不会导致整个系统的宕机。

比特股目前全网在线的服务器有 27 个，由于 DPoS 共识算法提供了较好的交易吞吐性能，理论上比特股的 TPS 可达 10 万，这也是比特股在技术上区别于其他区块链的最显著特征。比特股较好的 TPS 其实也是为了它的功能服务的。

在这里，我们能看出比特股平台的性质。

首先，比特股平台是一个交易平台，交易平台的显著特征是整个市场对时间敏感，大家都希望下单之后快速成交，所以高 TPS 是一个交易平台的基本需求。

□其次，比特股是去中心化的交易平台。目前流行的中心化数字货币交易平台最大的问题是资金管理系统和撮合系统都由同一家控制的。

然而在传统的证券交易领域，证券登记和交易撮合是两个不同的主体，他们之间是协作关系，共同受到证券会的管辖。

所以，如果你的数字货币□存在中心化交易平台，你的交易撮合也□受它来控制，这里的交易撮合指的是一个交易双方通过挂出买单和卖单，系统完成撮合匹配直至最终成交的过程。

由于以上的这一切都是不透明的，这里面就有很多的不确定因素。

比如交易平台跑路风险、黑客攻击、资产莫名其妙丢失，或者撮合的过程中，交易对手方是谁，是否有内幕交易。这些情况都会带来较大的风险。

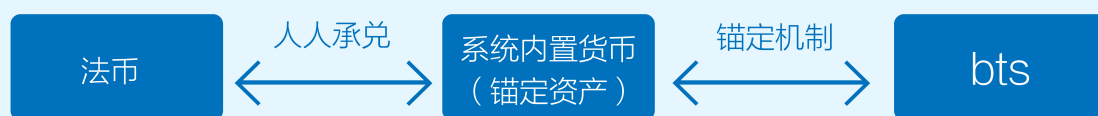
## 比特股的两个机制

那么比特股是如何设计中心化交易所来避免上述风险的呢？

比特股作为一个去中心化的交易所，它有两个机制可以避免上述的风险。

第一、资金出入是由承兑商来支持的，人人都可以成为承兑商，也就是人人承兑；第二、锚定机制提供了稳定货币的出入金过程，锚定机制也保证了比特股的出入资金和交易撮合是分离的，避免了中心化交易平台的弊端。

这个过程可以简述为：法币 <—> 锚定资产（系统内置货币） <—> btc 的相互转换。从法币到系统内置货币用到了人人承兑机制，从系统内置货币到 btc 的转换用到了锚定机制。



这里的 btc 是比特股上流通的平台代币，它和比特币一样有类似的总量上限设定，大约在 36 亿左右，目前流通量 26 亿左右。我们接下来就来看看这两个机制。

## 1. 人人承兑

人人承兑就是提供了从法币到系统内置货币的转换，比特股系统内置了多种货币，它锚定了多数法币。

例如 bitCNY、bitUSD、bitEUR 等等，这些系统内置货币是可以与 CNY、USD、EUR 按照 1: 1 兑换的。而人人承兑货币其实就是提供了 bitCNY 和真正人民币之间的相互转换。

它的机制上有点类似那个比特币的场外交易。所谓场外交易，就是没有中心化撮合中介，交易双方自行议价成交。

例如，我想要买比特币，就可以找到一个专门的承兑商，直接把这个钱支付给交易商，然后承兑商再把比特币支付给我。这部分的内容，后面我们讲数字货币交易所的时候会和你详细讲解。

人人承兑□在逻辑上差不多，它提供了一个 CNY 法币和 bitCNY 的兑换手段，实际上就是让法币和□比特股系统内置货币的交换能够进行，而且是去信任的进行。

所以从资金托管的角度来看，比特股与中□心化交易所很大的区别，比如你在一个交易所里充值，你只能信任这个交易所在保管你的钱，在你要提现的时候，你只能信任交易所□愿意让你提出。

但是人人承兑的就不一样了，人人承兑是你从 A 承兑商获取 bitCNY，你可以找 B 承兑商再换成人民币，不需要只在同一个地方兑换。

因此一个人此时有充值的需求，过一段时间可能就有提现的需求，所以实际上每个人都可以成为承兑商，□我可以是买家也可以是卖家，交易角色的转换可以让市场更灵活。当然市场上也有专门提供充值和提现服务的“承兑商”，这些承兑商收取手续费来盈利。

但是，不是所有的中心化风险都可以通过技术解决，人与人的信任问题没有一劳永逸的解决办法，即使你们当面交易也有可能遇到对方欺诈的行为。

我们只能说，CNY 法币与 bitCNY 锚定之后的充值和提现相对更安全，人人承兑提供了一种有效的机制，缩短了出金入金的周期，提升了安全性，如果资金在比特股系统之内，整个使用期间也没有人能威胁到你的资产。

## 2. 锚定机制

锚定机制是一种去中心化的抵押机制。我们刚才提到了比特股系统内置了多种货币，它锚定了多数法币，例如 bitCNY、bitUSD、bitEUR 等等，这些系统内置货币是可以与 CNY、USD、EUR 按照 1: 1 兑换的。

系统内置货币的发行商是系统自身，发行给抵押了 bts 的用户，发行的数量是由抵押的代币数量决定的。你用 bts 抵押，然后换取 bitCNY。

换句话说，任何持有 bts 的人可以用它来抵押生产系统的内置货币，例如 bitCNY，它的抵押规则要求两倍□价值的 bts 进行抵押，由于有 2 倍价值的 bts 作为保障，所以定义 1 bitCNY = 1 元人民币的风险较低。

比特股系统本身提供 bts 与 bit□CNY 交易对，例如现在 bts 价格是 0.5 元人民币，我就能用 4 个价值 2 元的 bts 抵押产生 1 枚 bitCNY，也就是 2 倍价格抵押。

这种抵押担保机制保障了 bitCNY 的价值，并且从技术层面来讲，比特股的共识机制保证了恶意修改 bitCNY 的数量的造假行为是不可行的。

如果 bts 价格下跌，系统就会自动把我抵押产生的 bts 卖掉，因为抵押了 2 倍价值的 bts，所以如果没有暴跌 50% 以上，系统都可以在交易市场上卖掉我抵押产生的 bts，并在市场上获得 bitCNY。

如果暴跌 50% 以上，系统会以一成的价格（强制平仓）卖出抵押的 bts，直至卖够抵押产生的 bitCNY。

从操作层面来看，支付 bitCNY 实际上消耗的还是 bts，但需要消耗多少，就以实时价格买入多少 bts。

买入操作是瞬间完成的，在比特股上有专门的代币资金池来提供，实时价格由系统为之决定的，所以使用者不用承担任何比特股代币价格波动带来的风险。

至此，稳定的 bitCNY 货币就产生了，它兼具了区块链的优点，且是一种稳定货币。

除了抵押以外，还有强制平仓、强制清算这种机制来保证价值和实际所锚定的货币等价。内容比较深，留给你自己挖掘。

## 比特股的技术概览

比特股的核心代码是由 Cryptonomex 公司开源的石墨烯（Graphene）框架演变而来，它的主体代码是 C++ 编写的，里面使用了大量的 boost 库组件，如果你对石墨烯技术感兴趣，并且熟悉 C++，可以仔细研究一番。

除了比特股核心，这里还有一套 Javascript 编写的 UI 产品，叫做 Bitshares-UI，Bitshares-UI 其实是一个轻量级的基于浏览器的钱包：比特股钱包，这个钱包将用户密钥存储在本地浏览器上，并且密钥是通过用户密码加密并储存在浏览器数据库。

发送交易时，先本地对交易进行签名，再传输到代理服务器上，由服务器广播至比特股全网，这个服务器你也可以自己搭建。

比特股所使用的共识算法我们已经讲过，是 DPoS，所以比特股也有见证人节点，目前有 101 个见证人节点，从 101 个节点中，社区又选出了 11 位代表，我们叫做理事会。理事

会接受社区投票然后行使比特股上的治理权。

比特股使用的也是 ECC 椭圆曲线非对称加密算法，值得一提的是，比特股并没有类似比特币地址的概念，在比特股上取而代之的是可读的账号系统，这些账号与私钥一一绑定，可读账号就是比特股系统中的地址。

比如我的账号是“chenhao”，那么在比特股上，你支付给我 bitCNY 的时候，接收方一栏直接填“chenhao”即可。

## 总结

今天我向你详细介绍了比特股系统，比特股也是一场伟大的实验，它打破了区块链应用数字货币的局限性，让区块链技术具有丰富的金融特性。

比特股技术上的优势多体现在 DPoS 算法上，所以本篇我重点介绍了比特股的□产品特性。

比特股社区也是区块链界的一股清流，因为持有比特股往往需要学习大量金融知识。

投资者想要投资比特股，光是弄清楚锚定机制足以让投机者□就需要花费大量时间，所以一旦被比特股套牢，似乎只能学习比特股进行自我提升，这也让比特股社区的平均金融知识储备高于其他区块链项目。

比特股上的“强制平仓”和“强制清算”是什么意思呢？你可以跟我留言，我们一起讨论，感谢你的收听，我们下期再见。

附录：

1. 【<http://bitshares.org/>】
  2. 【<https://github.com/bitshares/how.bitshares.works/tree/master/developers#bitshares-documentation-for-developers>】
-



# 深入浅出区块链

你的区块链入门第一课

陈浩 元界 CTO



新版升级：点击「👤 请朋友读」，10位好友免费读，邀请订阅更有**现金**奖励。

© 版权归极客邦科技所有，未经许可不得传播售卖。页面已增加防盗追踪，如有侵权极客邦将依法追究其法律责任。

上一篇 第19讲 | 上手搭建一条自己的智能合约

下一篇 第21讲 | 引人瞩目的区块链项目：EOS、IOTA、Cardano

## 精选留言 (6)

写留言



宇

2019-03-19



如果暴跌 50% 以上，系统会以一成的价格（强制平仓）卖出抵...

极客时间版权所有: <https://time.geekbang.org/column/article/6834>

跌了50%以上，因为是两倍抵押，那么应该无论怎么卖都是亏的吧？



smith

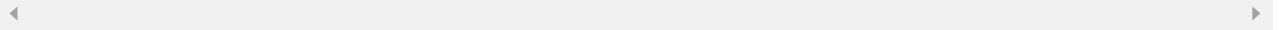
2018-06-12



27个服务器，理论上tps可以到10万，就是分布式架构，可以这样理解么？

展开 ∨

作者回复: 可以的, 多了代币在里面



**smith**

2018-06-12



理论上bts可以到10万tps, 其实就是分布式架构?

展开 ▾



**麻袋**

2018-06-06



蛮有难度的, 看来还要多阅读几次

展开 ▾



**奇雪人**

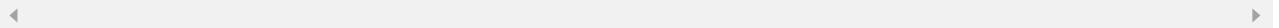
2018-05-10



锚定机制有点儿难理解呀...

展开 ▾

作者回复: 是的呀



**勇闯天涯**

2018-05-10



是不是可以通过学习比特股的金融合约代码来学习他的核心呢? 也加强对金融概念的了解

作者回复: 是的, 可以的哦。主要是抵押的概念

