BitShares 2.0 白皮书

一、高性能和可扩展性

每秒可以实现超过 10 万次转账

为了给业界提供一个有可能代替现有的金融平台的方案，高性能的区块链技术对加密货币和智能合约平台来说是必须的。为了能够实现比 VISA 和 MasterCard 加起来每秒可以处理的交易数量更高的级别，比特股从底层开始重新设计。通过股份授权证明机制，比特股网络可以在平均一秒的时间内确认交易，唯一的限制只是光速。

总览

要达到这个产业里面最顶级的性能，比特股借鉴了从 LMAX 交易所里面学到的经验。这个 LMAX 交易所可以在每秒内处理高达 6 百万次的交易。在这个经验里面，关键点是以下这些：

1、将一切东西放在内存里面

2、将核心的业务逻辑放到一个单线程里面

3、将加密算法操作（哈希和签名）放在核心业务逻辑以外

4、将校验的操作分成状态独立和状态依赖检查

5、使用一种面向对象的数据模型

通过遵守这些简单的规则，比特股在没有进行任何显著性优化工作的情况下就实现了每秒处理 10 万次转账的性能。如果有进一步的优化工作的话，会让比特股可以达到跟 LMAX 交易所相近的性能表现（即每秒 600 万次）。

应该需要注意到，比特股达到的性能表现是高度依赖其中的一个兼容交易协议。如果想用业务逻辑运行在一个进行加密算法操作和用哈希识别器去调用所有对象的虚拟机上的话，是不可能去达到同样层级的性能表现的。区块链天生就是单线程的，而单核的 CPU 的性能是各种资源中最短缺的、最难扩展的一个方面。比特股设计成能够让这个单线程的执行达到极可能的高效。

背景

区块链是一个下达关于确定去修改一个共享的全局状态交易的全球账本。这些交易中包含的命令可以改变其他交易的有效性。例如，你不能在你的支票存入生效前去从你的银行账户理解支取金钱。在能够影响一个特定的账户的所有先前交易都被处理之前，你不可能知道一个交易是否有效。

如果两个无关联的账号没有共享任何通用的依赖关系的话，理论上这两个账号的交易可以是在同一时间进行处理的。实际上，在一个由具备仲裁条件的智能合约驱动的账本上识别哪些交易是真正独立存在的耗费是很棘手的。唯一的保证两个交易是真正独立存在的方法，是通过维护完全分离的账本，然后定期在它们之间传输价值。如果要用这种性能表现的权衡关系去打比方的话，可以像是非一致内存访问架构（Non-Uniform Memory Access ，NUMA）和一致内存访问架构（Uniform Memory Access ，UMA）之间的关系。

实际上，一致内存访问架构对开发者来说是更容易去设计的，而且耗费更低。非一致内存访问架构通常是在建造超级计算机和大型计算机集群时作为不得已的方法去采用的。

计算机产业逐渐意识到通过平行计算去实现性能的扩张并没有早期那么容易，毕竟那时候最需要做的事情只是提高处理器的频率而已。就是因为这个原因，处理器的设计者们在尝试去采用多线程设去提高性能之前都在拼命去提高单线程的性能。当多线程还不够的话，而且只有这样的话，集群计算这个方案才会被考虑。

很多加密货币产业的人在没有探索过在技术上一台电脑的单个核心能实现什么之前，就尝试通过用集群计算的方案去解决可扩展性的问题。

LMAX Disruptor 分解器技术

LMAX 分解器提供了一个在单线程上可以实现什么表现的学习例子。LMAX 是一个针对终端顾客的交易平台，目标是成为世界上最快的交易所。它们一直很慷慨地将他们学到的东西公布出来。

这是它们架构的概要总览：

业务逻辑处理器是所有顺序交易和订单匹配发生的地方。它是一个可以每秒处理百万级别订单的单线程。这个架构可以很容易地用在加密货币和区块链设计的领域。

输入分解器扮演的角色是从很多来自不同源头的用户里面收集订单，然后分配给它们一个确定的顺序。当给它们分配好顺序后，它们会被复制、记录然后广播到很多冗余的业务逻辑处理器。输入分解器是高度并行的，而且容易分包到一个计算机集群系统中。

当业务逻辑处理器处理完输入后，一个输出分解器负责通知那些关心结果的人。这也是一个高度并行的任务。

最终，通过在业务逻辑处理器里使用单线程样品化处理器和 Java 虚拟机，LMAX 可以在每秒内执行 600 万次交易。如果 LMAX 可以达到这个成绩，那么加密货币和智能合约平台平不需要在每秒连 10 个交易都不到的情况下去考虑集群网络方案。

高性能区块链

要建造一个高性能的区块链，我们需要使用 LMAX 同样的技术。这是几个必须实现的事项：

将所有东西放在内存上，避免同步原语（锁定，原子操作），避免在业务逻辑处理器上不必要的计算。

由于内存的设计是高度并行的，因此越来越便宜。追踪互联网上每个人的账户余额和权限所需要的数据量是可以放在小于 1TB 的 RAM 内存上，这用不到 15000 美元的价格就能买到了，而且可以装在商品化（高端）的服务器主板上。在这个系统被 30 亿人采用之前，这类硬件会在普通的桌面计算机里面看到。

真正的瓶颈不是内存容量的需求，而是带宽的需求。在每秒 100 万次交易和每笔交易占 256 字节的情况下，网络会需要 256MB 每秒的数据量，即 1Gbit/s 的带宽。这样的带宽在普通的桌面计算机上并不是常见的。不过，这样的带宽只是二代互联网 100Gbit/s 带宽的一点而已。这个二代互联网被供应给超过 210 个美国教育机构、70 家公司和 45 个非盈利机构和政府机构。

另一句话说，区块链技术可以轻松将所有东西保存在内存里，而且如果设计的合理的话可以扩展到支持每秒百万级别的转账。

分配 ID 并避免哈希计算

在单线程系统的系统里面，处理器周期是需要被保留的稀缺资源。传统的区块链设计使用加密算法基础上的哈希计算去生成一个全球独特的 ID 系统，以实现统计学上不会有碰撞的保证。进行这些哈希计算的问题是，它会耗用越来越多的内存和处理器周期。与一个直接的数组索引相比，这种方式会显著地占用更多处理器的时间去查找一个账户的记录。例如，64 位的整数对比和操作起来都要比 160 位以上的 ID 更简单。更大的哈希 ID 机制意味着 CPU 缓存里面的空间更少了，而需要更多的内存。在现代的操作系统里不常访问的随机存储器是会被压缩的，不过哈希识别器是随机数，这是没法压缩的。

型号区块链给了我们一个在全球内分配独特的 ID 的方法，这些 ID 互相之间不会起冲突，因此完全避免使用像比特币地址那样的哈希算法为基础的识别器去引用一个账号、余额或者许可。

从业务逻辑处理器中去除签名校验

所有在加密货币网络的交易依赖于用加密算法签名去校验权限。大部分情况下，请求的权限可以由其他交易的结果改变。这意味着在业务逻辑处理器里面，权限需要被定义成与加密算法计算无关的情况。

要达到这个目的，所有的公钥需要分配一个独特的和不可代替的 ID。当 ID 被分配后，输入分解器可以校验提供的签名与指定的 ID 是否匹配。当交易到达业务逻辑处理器后，只需要去检查 ID 就可以了。

这个同样的技术可以在拥有不可代替的静态 ID 的对象上实现去除前提条件检查。

为静态校验设计交易

对交易来说，有很多特性是可以进行静态检查的，而不需要引用当前的全局状态。这些检查包括参数的范围检查、输入的去冗余和数组排序等。通常来说，有很多检查是可以被进行的，如果交易包含它“假设”是全局状态的数据的话。在这些检查被执行后，业务逻辑处理器必须要做的事情就只有去确保这些假设还是正确的，这个过程总结下来就是检查一个涉及交易签名时间的对象引用的修改时间戳。

智能合约

很多区块链正在整合一种通用的脚本语言去定义所有的操作。这些设计最终将业务逻辑处理器定义为一个虚拟机，而所有的交易被定义为由这个虚拟机运行的脚本。这个方案有一个在真实处理器上的单线程性能极限，并且由于将所有东西强制通过一个虚拟处理器去执行，让问题更严重了。一个虚拟处理器即使用上了实施编译技术（JIT）也总会比一个真正的处理器要慢，不过计算速度并不是这种“任何东西都是一个脚本”方案的唯一问题。

当交易被定义在这么低的层次上，意味着静态检查和加密算法操作还是会被包含到业务逻辑处理的环节里，这也让会让整体的吞吐量降低。一个脚本引擎永远不应该要求执行一个加密算法签名检查的请求，即使这个请求是通过原生的机制实现的。

根据我们从 LMAX 上学到的课程，我们知道一个为区块链设计的虚拟机应该考虑到单线程表现。这意味着在一开始就要为实施编译优化，而且最常用的智能合约应该通过区块链原生支持，而只有那些不常用的、定制的合约会运行在一个虚拟机上。这些定制的合约设计的时候要考虑性能，这意味着虚拟机应该将可以访问的内存范围限制到可以放在处理器缓存上的级别。

面向对象的数据模式

在内存中保存所有东西的其中一个好处是，软件可以设计成模仿现实世界中数据的关系。这意味着业务逻辑处理器可以迅速根据内存内的指针去找到数据，而不是被迫去进行耗费高的数据库查询任务。这意味着数据不需要复制就能访问了，而且可以当场就被修改。这个优化提供了比任何数据库为基础的方案高一个数量级的性能表现。

结论

设计一个高性能的区块链并不是什么火箭科学，而且既不需要复杂难懂的协议，也不需要在网络上的所有节点里分处理任务。反而，要建造一个高性能的区块链最需要的事情应该是在核心业务逻辑上去除与关键性、订单依赖性和评估无关的计算任务，并且设计一个可以帮助优化这些事项的协议。这就是比特股做了的事情。

二、自定义资产和身份管理

纽约证券交易所作为一个公司，它主要的职能是维护包含公司所发行股票或者债券所有者信息的账本。它主要的盈利方式是交易费用，以及它自己的股票等。

类似于纽约证券交易所，BitSHares 允许人们在系统中发行自己的股票或者债券，并且能够在一个分布式账本中进行交易。BitShares 能够在系统中标记每个账户来确保对应关系。这个信任网络能够让发行者在确保符合证券限制相关规定的情况下授权给其他人。

BitShares 平台能够提供一种称之为“用户发行资产（user-issued assets，UIA）”的特性，旨在帮助推动能够让一些针对某些服务的盈利性商业模式能够整合进入平台。UIA 本质上是一种注册在平台上得某种凭证，它能够在遵守某些特定要求的情况下在平台上进行交易。凭证的创造者可以设定 UIA 的公开名称、描述等信息，并且根据自己意愿来发行它。发行者业能自定义 UIA 的某些特性：例如可以要求只能允许在白名单内的用户才可以持有凭证，或者要求用户在转移或者交易这些凭证时需要支付一定的手续费。

例如，我们可以设想某个货币交易所是能够利用 BitShares 的交易引擎来提供它的交易服务。企业能够仅仅接受来自自己所认证的客户的现金，同时将相关 UIA 凭证存入客户在 BitShares 的白名单账户中。而这些客户能够使用 BitShares 的交易引擎来交易这些 UIA，当时发行者还能够收取到按百分比设定好的交易费。当用户完成交易需要提现时，发行者可以凭用户所持有的 UIA 兑换相应的货币可用户。这样，客户获得了他所需要的交易服务，同时企业也获得了交易费用，BitShares 平台能够尽可能的帮助双方变得更有效率，同时也可以获得自己的收益。

数字货币交易所和汇款机构可以发行自己的网关资产（UIA），这样可以在 BitShares 完成资金的进出。

企业可以直接在 BitShares 的区块链上发行自己的公司股票，而且这些 BitShares UIA 能够设定为完全符合现有监管和相关法律条文。

UIA 还可以用来作为奖励券，优惠券，第三方货币，信贷，产品收据，众筹凭着，保修凭证等等。

那些希望能够在 BitShares 网络上发行自己的股票或者债券的企业，需要支付一小笔费用给来保留其股票代码。这些企业能够自己定义相应的规则和手续费，完全按照自己的要求在 BitShares 展示和交易 UIA。

去中心化资产交易所

BitShares 会提供一个具有极高性能的去中心化交易平台，能够提供一切你所希望在一个交易平台上应该具有的功能。不仅订单的执行在你提交的瞬间就能够完成了，并且还能提供抵押债券让你能够使用杠杆和提供利息，期权合约能够让你对冲你的仓位。

中心化的交易所已经一次又一次的让世界知道它们是多么的不可靠和不值得信任。无论是 MF Global，Mt. Gox，或者是 BitStamp，让我们可以看到如果让第三方保管你的钱会发生什么。无论它们规模有多么庞大，有多少审计、监管机构或是保险公司，那些全球中心化的银行和交易所还是每天都充斥着各种欺诈、滥用职权或者盗窃行为。现在应该到了改变这一切的时候了，在这里可以让我们看一下全球首个全功能的去中心化交易所，BitShares。

去中心化

去中心化让 BitShares 面对失败时具有鲁棒性（Robustness，指原始载体在经历各种信号处理过程后，隐藏信息仍能保持完整性或仍能被准确鉴别，不因处理攻击后而导致秘密信息丢失的能力）。当一个中心化的交易所被泄露数百万美元将会瞬间影响数千个用户。而一个去中心化的系统被攻击或者出现故障只会影响单个用户和他的资金。用户能够控制他们自己的安全性，这其实可能远比任何中心化实体要好得多。

其实在试图破解一个交易所或者单个用户是存在一个固定成本的。这个区别就是在能够获得的收益大小。如果你花费数百万美元的成本来攻击一个特定的目标，那你肯定期望把这么多的精力放在一个交易所而不是你的单个个人账号。

在一个特定的公司里许多人都有机会可以接触到资金。你也许听到过俗话说“三个人守不住秘密，除非另两个不在人世”，大多数交易所都希望通过多个人来负责保护私钥的方式来控制资金。而如何其中的任何一个人出现问题，则每个人的资金都会是危险的。在这方面，事实上每个人独立负责守护自己的密码可能要比多签名要安全的多。

快，但不会“太”快

随着 BitShares 的交易速度在几秒内就可以得到执行，这就已经和中心化的网站界面差不多了。这不像中心化的交易所，他们可以在高频交易中设置优先单或者隐藏单，而是把所有的交易者放在一个公平的竞争环境中。

那些华尔街交易所会尽可能想办法在物理位置上接近交易所，是因为他们自动交易机器人的速度已经快到只有光速才能成为他们真正的限制。而在一个去中心化的交易所内，由于位置变得不再重要，于是的每个人都获得了平等的机会。

安全

美元，欧元，比特币和黄金，在 BitShares 交易所中都有着三倍于传统中心化交易所的资产支撑。那些传统的银行体系，其实应该被称为“虚构储备银行体系”，也常常称为“部分准备金银行体系”。在比特币的生态系统中，我们常常要求能够至少提供 100%准备金。即使这些交易所能够做到，但是一次被黑客攻击、错误或者被盗窃都很容易让这个 100%准备金系统变成一个虚构准备金系统，或者，有时候更糟糕的成为了“没有准备金的系统”。在没有任何准备金的情况下，是不可能让这些交易所把你的钱还给你的。

通过始终保持至少 200%以上的准备金的情况下，你可以放心，BitShares 在任何市场中都将具有偿付能力。所有准备金都会以 BTS 的形式安全的存放在区块链上，这样它们永远不会被盗取，因为没有人能够获得偷窃这些准备金的私钥。

无限制

你可以在任何时间，从任何地方，交易任何金额，而且没有提现限制。所有其他合法合规的交易所，每天提现的限制大约都是数千美元的数量级。如果你想超越这些限制，你必须提供许多文件来提升你的等级。一些交易所，如 Coinbase，甚至限制了你的钱在提现后只能用于哪些方面。还有一些其他交易所要求你提供文件来证明你是如何获得这些数字货币的。

随着 BitShares 的出现，你的帐户不再需要任何人的批准，你将会获得完整的财务自由。

收费低

因为每笔交易只需几美分，BitShares 肯定是全球成本最低的交易所。其他交易所会根据你的交易量来收取一定比例的费用。对于 1000 美元左右的交易，在 BitStamp 上你将支付 5 美元，而在 BitShares 上进行类似的交易收取的费用不到 0.01 美元(2015 年 1 月)。比较传统的交易所，如 ETRADE 或 Scottrade 平均每笔交易将会收取 5 美元以上，它们都不可能会比 BitShares 更加便宜。

交易一切

在这里你可以交易金，银，天然气和石油，还包括你所喜爱的国家法币和数字货币，在 BitShares 交易所上几乎没有任何限制。BitShares 交易所可以支持资产包括股票，债券，指数或通货膨胀(Inflation)。公司可以在 BitShares 网络上发行自己的股票，不仅方便，成本低，而且能够对保护交易来防止裸卖空。还有什么其他数字货币交易所能够让您进行黄金和白银的交易？了解更多关于 BitShares 系统是如何创建无需信任的数字资产来锚定几乎所有的东西。

从金银上赚取利息

还有什么其他的银行或交易所会为你的金银支付利息呢？随着 BitShares 每一个美元，欧元，比特币和其他资产将支付你一个积极的收益率可能是相当显著如果市场非常看好 BitShares。

开放源代码和完全透明

整个交流是开源的，由一个非常开放的社区支持。没有别的地方会让你有透明度，可与 BitShares 发现的水平。

隐私

通过使用 BitShares 你可以能够对隐私进行保护。就像比特币一样，所有交易都是完全公开但无需绑定到你的真实身份。不需要国税局文件，没有人会要求你的护照的复印件，驾照，水电费以及信用报告。

期权

不仅仅可以完成传统的交易，还可以买卖期权合约来帮助对冲你的仓位。所有期权合约完全抵押没有违约风险。

保证金和卖空

如果你想要一些杠杆来增加你的收益，BitShares 能够使您借贷和出售任何东西，包括美元、黄金、白银或者比特币等等。所有保证金头寸需要 300%的初始保证金和 200%的维持保证金，而没有进行信用检查的必要。

银行业的未来

BitShares 目前继续在高速发展中，随着这些特点和优势的出现，我们显然已经能够遇见银行业的未来。我们最终有了一个去中心化的，无需信任的的交易所，它能够和任何中心化的交易所已经运作而不用再去考虑它们是否会倒闭。如果你对研究 BitShares 是如何运作有兴趣的话，推荐可以看一下“未来的数字货币交易所”。

当 BitShares 着手开发时，著名的比特币交易所 Mt.Gox，它在美国银行的账号正在被冻结。从那之后，数家主要的数字货币交易所被黑客攻击或者倒闭。就在数周前，很有名的比特币交易所 Bitstamp，它的热钱包被泄露而导致暂停服务。这一次又一次的提醒我们，只要是我们通过第三方来保管我们自己的财富那就会有风险。今天我们希望通过 BitShares 来为人们提供一种全新的数字资产交易所。

想象一下，如果有一种交易所能够让你在购买和出售数字资产时完全无需承受接触对方而带来暴露隐私的风险。想象一下，如果一个交易所能够提供非常低的交易手续费，并且没有任何充值和提现金额限制。想象一下你可以在交易中使用任何一种货币，甚至包括黄金和白银。想象一下如果能够提供市场中最好的流动性。这就是 BitShares，这是数字资产行业中最棒的交易所，也是我们的秘密武器。

交易所的角色

在我们深入探讨数字资产交易所在将来是如何运行之前，先让我们回顾一下传统交易所在今天社会里是扮演那些角色。

1. 收到数字货币来发行 IOU（欠条）
2. 收取法币来发行 IOU
3. 处理订单撮合
4. 赎回 IOU

这其中的每一个角色都需要高度的信任，并且将直接面临对手风险（对手风险：交易中对方不履行其金融义务而产生的风险），因为你其实所交易的都是来自交易所发布的 IOU。为了更够获得更好的流动性以及更低的价差，大多数人都会逐渐集中在少数几个核心交易所上进行交易，于是每个人都面临同样的对手风险。作为大型交易所之一的 BitStamp 就是个很典型的例子，我曾经就有数千美元被系统锁死完全无法使用，因为似乎当时系统宕机了。

当资金进入或者提出交易所时往往需要等待很长时间，这意味着交易者这段时间内资金将会停留在交易所。这会显著放大交易所用户的风险，同样也会放大比特币生态系统所有用户的风险。每当交易所被发现出现巨大的安全漏洞时将会出现巨大的抛售压力，此时偷币的黑客会希望快速卖出他们所偷的币，而普通用户也希望能够在黑客抛售前出售。

中心化会侵犯隐私

数字货币是依赖于一个完全公开的账本，由于每个人都可以看到每一笔交易，能就让保护隐私成为一个不小的挑战。每个比特币用户可以有一个或者多个账号，这让每个使用者会有个错觉，人们认为只要别人不知道你的账号，而且进行每笔交易时都可以使用一个全新的账号，这样没人可以把你的真实身份和你的比特币联系在一起。

但是大型的中心化交易所却会影响到隐私保护的效果。为了遵循政府的监管要求，他们必须要了解每个人具体的账号信息。由于几乎每个人的交易都需要通过这样的交易所，那么交易所很容易知道每个人究竟是如何进行交易，并且对方是谁。目前 Coinbase 已经关闭了一些他认为在进行违规交易的比特币账户。

如果我们想拥有一点的隐私，甚至半点，恐怕你就需要在数百个第三方应用中很好的识别并且区分交易所的应用。然而这并不是一种很有效地方式，特别是大量市场交易会自然而然的倾向于越来越集中在几个中心化交易所上。

如果隐私问题对你很重要，我建议你看一下这篇文章《如何使用 BitShares 保护你的隐私》

权力分散

并没有什么必然的理由需要一个实体同时来发布 IOU 并且来处理挂单交易。之所以这两个角色会结合在一起的原因就是，我们倾向于将业务集中在比特币交易所。如果我们想要建立一个去中心化的交易所，那么第一步就应该把这些挂单账本放在区块链上，让每个人都可以看到。

交易所应该成为仅仅接受美元和在区块链上发行网关美元。当然他们收到网关美元之后，他们就应该马上把美元电汇给用户。他们全部的收入应该就是来自于手续费，而不是一定比例的市场交易费。可以看一下之前的文章来来了解一下是如何成为 BitShares 网关的。

区块链应该能够让用户在 BitstampUSD 和 BitfinexUSD 之间进行交易，这样资金就能够容易的从一个网站到另外一个。用户甚至可以在 BitstampUSD 和 BitStampBTC 或者 BitstampUSD 和 BitfinexBTC 之间进行交易

不幸的是，简单的在区块链上的账本进行移动是不够的，因为市场会围绕着几个网关 IOU 越来越集中化。BitstampUSD 不能和 BitfinexUSD 进行互换是因为互相信任和监管上得考虑。这些 IOU 都是有潜在违约的可能，就像那些在交易所内部数据的欠条一样。我们所需要做的就是把从对个人的信任转移到区块链。

有抵押的区块链 IOU

比特资产（BitAsset）系统是 BitShares 最核心的部分，它在 BitShares 的系统中通过建立 300%的抵押来创建。BitUSD 除了能够拥有 BitUSD 所有的特定，并且还能够有美元稳定的价格。在任何时候，你都可以通过卖出 BitUSD 而获得价值约 1 美元的 BTS。而在任何时候，抵押品的价值低于某个点之后，区块链会自动买回 BitSUD，并且返还价值 1 美元的 BTS。

只要 BitShares 它本身在合理的价格波动范围内，那你持有 BitUSD 时，它的价值将会一直锚定美元。这里所说的合理范围，已经囊括比特币在整个它生命周期内所出现过的最大波动范围。即使 BitShares 价格在 24 小时内跌至开始价格的 1/3 也不会有什么问题。那些目前已经被广泛使用的数字货币还没有出现过这么大范围的价格波动。这意味着除非是 BitShares 本身协议和软件出现了问题之外，否则没什么能够影响 BitUSD 的价格。

当你把你的持股 BitUSD 的价值将继续只要 BitShares 本身具有合理的波动与美元挂钩。当我说合理的，我的意思是它可以处理比比特币已经见过它的续航时间出现较大波动。 BitShares 的价格必须下降到不足 1/3 的起拍价在不到 24 小时，然后呆在那里。不合法的，广泛采用的加密货币已经见过那种价格变动。这意味着，BitUSD 是安全的反对几乎一切，但在 BitShares 协议本身就是一个无法修复的软件错误。到时候 BitShares 成熟的水平比特币是在今天，你可以期望的那种错误的概率是相似的比特币具有那种错误的。

如果你想了解更多关于我们系统是如何通过市场来锚定住 BitAsset 机制，请参见讨论该机制的详细文章。

全球统一的挂单账本

一旦市场能够接受 BitUSD 和 BitBTC ,并且将它作为一种比 BitStampUSD 和 BitfinexBTC 更为可靠的货币进行使用后，就会发现许多的交易量会朝着 BitUSD 和 BitBTC 开始转移。仅仅只有当人们要把现金转移到传统银行体系时，才会有人有意愿将 BitUSD 转为 BitstampUSD。

当出现全球统一的挂单订单最终将会结束一切的套利机会，并且会减少利差，并且最大限度的提高流动性。由于大家都是通过 BitShares 网络执行交易，那么可以将避免高频交易和隐藏优先单之类的问题。高频交易和隐藏优先单都依赖于中心化的交易所巨大的交易量和市场深度。如果某些主要交易活动开始向去中心化和无需信任的交易所开始进行转移，那么那些中心化交易所剩下的交易量恐怕将不再能吸引太多的高频交易者。

更低的市场交易手续费

BitShares 会从每笔交易中收取手续费，就像比特币一样。目前每笔交易收得手续费少于 0.01 美元，这意味着你将 1000 美元转成大约 3 比特币只需要 0.01 美元。如果你打算在 Bitstamp 上做同样的事情你将会被收取约 0.5%或者 5 美元。从这一点来看，BitShares 大约要便宜了 500 倍左右。这也意味着相对传统交易所，由于更低的摩擦将会获得更多的交易。For allpractical purposes the fees saved here should cancel out any extra feesassociated with the BitUSD / GatewayUSD spread.

BitUSD 到美元的网关们

许多网关会更喜欢一兑一赎回这种低风险的做法，这只会让网关美元在兑换 BitUSD 出现一些小的浮动。最终，当用户通过网关美元从 BitUSD 兑换成美元时，将会支付一笔小且会变化的转换成本。

而另一方面，很多用户都希望直接将 BitUSD 兑换成法币美元。在这种操作模式中，网关需要提供一个固定百分比金额的交易手续费来提供所有的流动性。网关会试图通过提供尽可能低得费率来进行竞争。

在这种情况下，实际上 BitUSD 和美元加上一小笔固定手续费具有同样地效果，而且这个手续费也并不会比现有交易所的充值/提现费用更高。BitShares 将会有许多银行合作伙伴来提供全功能的交易系统，并且有没有任何限制。在任何时候时候，用户在系统中得资产都不用担心出现违约、被交易所或者网关没收。一个真正的去中心化交易就应该实现或完成 BitShares 最初的设想。

三、推荐计划

BitShares 将会是第一个内嵌推荐系统的区块链技术应用，旨在希望能够让系统用户获得几何级增长。如果推荐一个朋友来注册，将会能够获得未来他们 80%的交易手续费。传统的支付公司平均每获得一个用户大约需要 100 美元 ,许多公司即使可能没有非常明确的资金奖励计划也愿意为获得每个用户支付 40 美元。BitShares 主要是将大部分收入交给那些能够带来新成员的用户们。

如果你愿意加入 BitShares，并且成为一名**终身用户（Member）**那将会获得许多的好处。其中的福利有，所有交易费用将会以 80%现金返回，批量折扣，并且那些你带来的用户们，你有机会获得 80%他们的交易费用。我们预计对于每个长期用户将会产生超过 100 美元（注 1）的交易费用，那么你有可能在每个用户上获得超过 80 美元。成为 BitShares 终身会员的成本大约是 100 美元，这会非常容易的进行支付和推荐奖励。

工作原理

每一个新的帐户必须由现有的帐户创建，之所有需要这个要求是为了让现有账号能够支付账号注册手续费用。那个支付这个手续费用的人就是**注册者（Registrar）**。一般来说，这个**注册者（Registrar）**很可能就是钱包服务提供商。如果任何人注册成为**终身用户（Member）**，他们就有权划分推荐收入和一个可选的**推荐者（Referrer）**。如果注册者没有支付成为终身会员，新的账号将会继承注册者账号的推荐配置。在任何时间，每个账号都可以通过支付大约 100 美元（注 2）来升级成为一个终身会员。当一个账号成功升级后，100 美元的升级费用将会被划分给注册者和推荐者，账号变成“它自己的推荐者”。当一个账号是它自己的推荐者，那么他就会获得每次交易 80%的现金返还。

例子

让我们来看看这个系统在实践中是工作的一个例子。山姆在谷歌搜索“去中心化交易所”，知道了 BitShares 之后决定创建一个帐户。他选择了一个钱包托管提供商，例如在 moonstone.io 上创建一个帐户，而此时 moonstone 已经是终身会员，所以当萨姆在 moonstone 创建一个帐户之后，它设置的**注册者（Registrar）**和**推荐者（Referrer）**自然就是 moonstone 的账户。

在尝试了这项服务，山姆觉得他喜欢它，并且从长远来看成为**终身用户（Member）**会更加节省资金，并收取 80%的现金返还他所有的交易费用。于是他决定支付 100 美元的费用来升级成为**终身用户（Member）**，该费用是 BitShares 网络（20%）和 moonstone（80%）之间进行分配。

此时 moonstone 通知萨姆，他可以参加他们的联盟计划。每当萨姆引领到一个新的用户创建一个帐户，moonstone 将与山姆分享引荐收入。Moonstone 在它的联盟内分享它的引荐收入多少完全取决于 Moonstone 自己，但在这个例子中，我们假设是 50/50。

山姆挺喜欢这种方式，于是将 Moonstone 推荐给他的朋友爱丽丝。爱丽丝创建了 Moonstone 的帐户和并将 Moonstone 设置为**注册者（Registrar）**，而山姆被设置为**推荐者（Referrer）**，那么 Alice 今后每笔交易手续费 40%将会成为山姆的收入。如果 Alice 最终决定升级成为**终身用户（Member）**，那么她交支付 100 美元的手续费用，这笔费用将会分配给 BitShares 网络（20 美元），Moonston（40 美元）和萨姆（40 美元）。

条款及细则

请参阅推荐计划 - 合同条款和条件的更多细节。

1.此估计取决于类似 Paypal 和 Dwolla 公司愿意支付多少费用来获得客户和假设用户将在一生中至少进行 500 次交易。

2.实际的升级费用将取决于价格每日都会波动的 BTS。BitShares 的代表们将倾向于把 BTS 注册费调整接近 100 美元左右。

四、病毒推广计划

通过快速扩大用户群来鼓励大规模被使用

BitShares 已经在系统中内置了一个先进的推广程序。金融网络的价值主要来自于参与网络效应的人越多 ,那么对这些用户而言 ,这个网络的价值越大。BitShares 将会通过完全透明和自动化的方式，奖励那些能够吸引新人来注册的用户，而这些新人应该一些会是真正愿意使用该系统的用户。每带来一个的新用户，你有机会可以赚 80 美元或更多。

促进基础设施发展

该 BitShares 推广计划旨在促进基础设施的发展。所有的去中心化金融网络都取决于许多商业合作伙伴来共同建立一个生态系统。这意味着需要激励创业者来建设基于整个网络系统的商业模式，例如交易所、商户服务、钱包服务、轻量级钱包，以及区块浏览等服务。随着 BitShares 推广程序的出现，商户们能够通过宣传推广他们使用 BitShares 平台的服务，而获得显著受益。不像其他一些平台仅仅提供“更低手续费”，BitShares 商户将会提供一个全新的收入来源。

自由市场竞争将导致许多不同的托管钱包服务提供商，通过竞争来争取获取更多的新用户。这些提供商有可能用传统金钱激励方式来宣传他们的钱包，这也意味着将会快速扩大 BitShares 的网络效应。

背景知识——PayPal 的推广系统

建立引导一个新的金融网络是非常困难的，这通常会是一个先有鸡还是先有蛋的问题。一开始很难吸引新用户，因为新用户往往只会在有许多现有用户的情况下才会加入。

我们可以看一下像 Paypal 这样的公司是如何通过解决这个问题来达到临界点的。

PayPal 当时最大的挑战就是获得新客户。他们尝试着做广告，但是太贵了。他们尝试着商务发展（BD）来进入大银行，但是官僚作风太严重。PayPay 团队得出了一个重要结论：BD 无效。他们需要一种爆发式，病毒式的增长。它们需要给用户钱。

于是他们就这么做了。新客户在注册后能够获得 10 美元，而推荐新客户的用户也会获得 10 美元。于是开始爆发式增长，PayPal 还将提高到为每个新用户支付 20 美元。这个方式让人感觉既有效又无效，每天 7—10%的增长，以及上亿的用户让人感觉非常棒，但是没有收入和爆炸式的成长则不怎么令人开心了。情况看上去有些不稳定。PayPal 需要开始制造影响来筹集更多的钱并且继续推进下去。

给客户钱是一种非常昂贵而且不是太容易持续的方式，但是它被证明非常有效。

获取客户的成本 VC 客户生命周期价值

BitShares 认识到要一个可持续发展的系统，必须能够从现金流中获得可以覆盖所有操作的费用。这里有一篇名为“初创公司杀手：获得客户的成本”的文章节选，作者 David Skok，这是他在通过观察了数百个失败的初创公司后所分享的经验。

然而通过近距离观察了数百个初创公司是如何失败之后，我注意到非常多的团队其实都已经成功解决了产品/市场的匹配问题，但还是失败了，就是因为它们没有能够找到一个通过足够低成本方式来获得客户。

一个非常平衡的商业模式必须是，获得用户的成本远低于其客户为企业所创造的利润。

对于像 BitShares 这样的例子，交易费用需要设置的足够高来足够覆盖所有成本，包括获取用户的成本，同时还要足够低到能够面对那些现实中的竞争对手。大多数的数字货币网络很少能够通过交易费来覆盖整个网络运行的成本。它们往往会试图通过低手续费来吸引客户。尽管低手续费也很重要，但是低质量的服务反而适得其反。因此 BitShares 对于交易费可能会高于某些数字货币网络，但肯定会远低于那些传统交易所，并且提供像 Dwolla 或者 PayPal 这样的支付网络。

为了确保客户获取成本是可持续的，BitShares 推广制度被设计成为能够按实际收益的百分比来进行支付。对于关于每个所推荐用户的生命周期价值（ Life Time Value，LTV) 这个问题， BitShares 将会让用户们自己得出他们的结论，他们也可以自己去研究一下相似行业客户的 LTV。我们认为 BitShares 网络在当推荐者每成功引荐了一个新用户时，提供大约 80 美元的奖励，或者如果是下线的话提供大约$40 美元的奖励。当然，这个奖励必定是基于是真实用户在使用系统服务的情况下。即使一个客户被我们高估了 4 倍，BitShares 仍提供比 PayPal 更多的激励。

结论

BitShares 构建的病毒式推广方式和业界领先的激励方案将会改变游戏规则。