BitShares
比特股

点对点的多态数字资产交易系统

A PeertoPeer Polymorphic Digital Asset Exchange

Daniel Larimer
dlarimer@invictusinnovations.com
www.tradebitshares.com

Charles Hoskinson
charles.hoskinson@invictusinnovations.com

Stan Larimer
stan.larimer@invictusinnovations.com

翻译:暴走恭亲王　巨蟹

注意:本白皮书正在积极修订中，非常欢迎来自您的意见。

摘要

一个理想自由市场金融体系（Ideal Free Market Financial System，IFMFS）应当允许参与各方在最小化风险和成本的前提下，对价值进行存储、交易和转让。在基于比特币首次所提出具有开创性的开源协议之上[1]，我们进行了改进和扩展，重新定义了一个新的名为比特股（BitShares）的协议，以用来实现一个理想自由市场金融体系。在比特股网络当中，我们创造了一种新的名为多态数字资产（Polymorphic Digital Asset，PDA）的金融产品。它能够跟踪黄金、白银、美元或者其他货币的价值，并且让持有者获得红利的同时避免所有的交易对手风险。比特股拓展了比特币的技术，在一个全新的点对点的多功能网络中，提供了很多传统货币功能，以及能够让比特币和其它常见金融资产共同使用的支票账户、储蓄账户和证券经纪工具。

比特股网络提供的价值一部分与比特币源自同样的需求，另一部分则源自一些新的需求，这些需求包括：

1、对数字化的、可替代的、可分割的、可匿名且无需授信资产的需求；
2、对价值的安全存储需求；
3、对和风险成正比的投资回报需求；
4、对一个自由开放的交易市场的需求。

无论是作为储值手段还是高效交易系统，比特股成功的关键要素就是被广泛使用，为此，比特股尝试提供对每一个人都有充分吸引力的收益，以补偿使用比特股带来的技术的，社会的，监管的和政治上的风险。

---

[1] 请参考中本聪的白皮书：http://bitcoin.org/bitcoin.pdf

导言

比特币带来了互联网商务的革命，它使安全的，私密的，且不附带交易对手风险的价值交换成为可能，比特币证明了一个去中心化的数字资产可以实现基于算法的供应量限制，持续升值，以及无需任何物理或政治背书的高效交易。

不幸的是，比特币，就像其他所有现存的加密货币一样，受制于价格波动和低流动性，同时也无法方便地在一个透明的全球性市场上与黄金和美元等资产进行交易，用户必须借助于中心化的交易所和清算中心才能买卖加密货币，这阻碍了主流人群对加密货币的接受。我们的目标是拥抱比特币带来的创新，同时在不引入授信机制并且不需要对现存加密货币交易所进行重大改动的基础上，实施多项革新以解决加密货币的价格波动和低流动性问题，我们的解决方案就是比特股（Bitshares）。

理想自由市场金融体系的特性

我们首先讨论一个理想自由市场金融体系的性质。从建立它的动机开始到需要的原则。我们目的是发展出一个能够为比特股和竞争对手共同借鉴的基础。

建立IFMFS的动机

我们需要一个数字化的自由金融体系，可以让任意种类的资产进行交易而无需毫无价值的中间商或者中心化的资产发行人[2]。事实上，我们希望在尽可能减少有问题的中央节点，监管规定和授信需要的同时，尽可能保留他们的功能。努力让市场超越地理和主权操纵的限制，并且可以让传统的交易所和金融服务机构整合进来而无需考虑当地具体的法律和监管问题。

理想自由市场金融体系的原则

通过慎重考虑和共同审核，我们选取下面的原则来定义一个IFMFS的特性，从而确定比特股网络的基础目标。

去中心化原则（**Axiom of Decentralization**，**AoD**）

参与IFMFS的各方享有同等的地位，不需要任何的特权，任何一方在任何时间点都不得要求尚未被超过50%的人群所拥有和使用的资源。

信任原则（**Axiom of Trust**，**AoT**）

参与IFMFS的任何一方都不需要相互信任。没有一方可以违约，并且不应该以合同义务作为先决条件。

---

2 Bernard von NotHaus“自由美元”案例展示了中心化的发行人来发行金融产品而无视工具的困境:

http://www.nytimes.com/2012/10/25/us/libertydollarcreatorawaitshisfatebehindbars.html?pagewanted=all&_r=0

责任原则（**Axiom of Liability**，**AoL**）

在IFMFS中没有任何一方需要从事非法或高度管制的活动，或者承担超过和朋友或家人进行加密货币与法币直接兑换的法律风险。

易用性原则（**Axiom of Accessibility**，**AoA**）

一个IFMFS应该足够易用，使任何有能力使用电子邮件的人都能掌握并且成功地在系统中交易获利。

可扩展原则（**Axiom of Scalable**，**AoS**

一个IFMFS必须能够在不损害系统其它原则，也不需要引入其他中心化的参与者的前提下扩展至任何量级的处理能力。

资产和交易的多样性原则（**Axiom of Asset and Trading Diversity**，**AoATD**）

一个IFMFS应该支持常见的投资工具，包括买空卖空，认购和认沽期权。它应该支持对任何有形资产的交易。

聚集原则（**Axiom of Aggregation**，**AoAG**）

在IFMFS中，一个单一的买单应该可以匹配多个最小交易单位的卖单。一个试图进行大额交易的用户只需发起一笔交易。

原子性原则（**Axiom of Atomicity**，**AoAT**）

在IFMFS中，没有一个交换或者交易是部分的，不完整的，或者处于无效的状态。

中介原则（**Axiom of Escrow**，**AoE**）

IFMFS系统外资产与系统内资产余额的交易不应依赖于对包括买方，买方或中介代理的任何一方的信任。中介系统应不易被买方或卖方与中介代理串谋攻击。

整体定价原则（**Axiom of Global Pricing [AoGP]**）

IFMFS不得使用任何非来自系统用户出价的价格信息。

零和原则（**Axiom of Zero Sum**，**AoZS**）

一个IFMFS必须既不创造也不毁灭价值，任何一方的盈利一定是建立在另一方的损失上。任何一方都不会有对系统的负债。（参看AoT）。

整体吸引力原则（**Axiom of Global Appeal**，**AoGA**）

一个IFMFS应该提供有足够吸引力的收益，而超越与之相关的风险，来促进每一个人参与，分享和推广，当与任何监管风险对照时，这些收益应产生深度最大的可能市场，最大的流动性，最广泛的公众支持，以及最大的需求。

隐私原则（**Axiom of Privacy**，**AoP**）

一个IFMFS至少能够为所有参与的用户提供和比特币同级的隐私保护。理想情况下，能够彻底匿名[3]。

赫尔墨斯原则（**Axiom of Hermes**，**AoH**）

一个IFMFS应该尽可能快的为用户处理存款，交易和提款。系统内的交易应该以最快的速度进行确认。

安全原则（**Axiom of Security**，**AoSEC**）

一个IFMFS必须拥有和比特币一样或者更好的安全水平。

开源原则（**Axiom of Open Source**，**AoOS**）

对一个普通开发者而言，所有IFMFS的相关软硬件必须是开放的，可审查的，可重新生成的。

---

3 我们已经就实现Zerocoin协议和采取一些其它措施来保护用户隐私作了很多讨论。更多信息请参考：http://zerocoin.org/。

被动订单执行原则（**Axiom of Passive Order Execution**，**AoPOE**）

订单可以在没有用户或他们的电脑的交互式参与的情况下执行。

据本文作者所知，到目前为止我们还没有发现一个系统同时实现这17个原则的系统。因此我们致力于开发一个简单而且优雅的系统来实现这些原则。本文将会描述我们是如何努力去实现的。

介绍比特股

比特股是一种多态数字资产，这意味着它可以演化成多种不同形态的比特资产（BitAssets）。比特资产的运作方式类似于比特币，但是一些优化和新的规则能够让比特股来支撑其价值。比特股除了拥有比特币的所有特性以外，还提供了一些新的特性使得持有比特股或者由比特股衍生的比特资产超过24小时后可以获取红利，这些红利来自于挖矿奖励和交易费用的一部分，会奖励给每个区块，并且以一种不增加网络负担的方式分发。

定义

红利（***Dividend***）—— 挖矿奖励和交易费用的一部分，按所拥有的比特股数量占已存在比特股数量比例分发。

比特资产（***BitAsset***） —— 一种有抵押的，由比特股以1.5至2倍或更高的保证金比例支撑的，拥有比特股所有可替代性，可分割性和可转移性的资产且可以获得红利的资产，所有红利由抵押物产生并以比特股的形式支付。

保证金（***margin***）—— 作为支撑的价值超过比特资产当前市值的资产。

比特美元（***BitUSD***） —— 一种由比特股支撑，价值通过自强制市场反馈机制与美元价值高度相关的资产。

比特***X***（***BitX***） —— 通用的命名比特资产的方式，基于自强制市场反馈机制与与之联系的资产实现价值相关（如比特黄金（BitGold），比特苹果股票（BitAPPL）等）。

块链（***block chain***） —— 一个全局同步的，区块结构的，有序的交易台帐。

输出挂单（***output***） —— 限定在特定条件下将如何被使用的交易台账余额。

交易***(Transaction)*** —— 将一组没有匹配的输出挂单和另一组新的没有匹配的输出挂单在满足输出匹配条件和其他块链规则的情况下进行匹配。

块链市场

交易算法和规则

块链的目的就是对全局交易台帐的事件顺序和当前状态建立共识。比特股需要这个全局台帐来建立转账，买卖和市场交易的顺序。每5分钟所有包含在上一个区块中的买卖挂单都会被匹配。

和比特币一样，每笔交易就是一组买卖输出挂单在一定条件下的匹配。主要的不同点在于允许形成交易的条件。（对比特股来说）这些条件包括：

1、由N签署的M私钥；

2、买卖挂单在指定交易汇率下被填充；

3、保证金到位；

4、回购比特资产以用掉剩余保证金；

5、认购或认沽期权在适当的价格被行使；

6、中介交易被发布；

7、中介交易产生争议；

8、中介交易争议被解决；

9、跨链交易的确认。

块链市场是价格信息进入块链的通道，保证价格信息准确且不受非基于市场力量的人为操纵是至关重要的，这些价格信息将被用来进行强制保证金追加。

用户可以自由的进行交易，交易记录将被记入块链，但基于个人之间达成一致意见的交易对于自动的价格发现是没有意义的，因为网络没有办法识别是否是同一个人用两个账户在进行交易。一次成功的交易必定是双方都同意的，同样，不成功的买卖挂单肯定是因为每个人都认为买方出价太低或者卖方出价太高。

那些不愿意进行“离链”谈判的用户可以将他们的买卖单放入块链当中。当矿工处理完接受到的所有交易数据时，他会把所有相容的买卖单按最高的买入价和最低的卖出价顺序配对。一旦所有能够匹配的交易完成，块链会将剩下未履行的买卖单列表。这些订单表示市场的共识价格在在买入价和卖出价之间。这个时候，会根据买入价检查所有空头仓位的保证金要求，所有保证金不足的空头仓位都会按当前卖出价进行强制平仓，保证金欠缺幅度最大的空头仓位将被首先平掉。

矿工匹配的买卖单中的资产项可以直到24小时的块链分叉窗口期过后才过账，因为如同coinbase交易，所有由矿工生成的没有拥有者签名的交易将不能在重组中被移入其它链，当你在达成交易24小时后依然不能在块链市场外过账资产项时，你可以在块链市场中下新的买/卖单让后续的矿工执行交易。

取消一个开放挂单也要遵守24小时的原则，因为一个块链重组如果发生在你下单之后和取消之前，可能造成其他矿工执行你的挂单。

创建比特美元

比特美元是一个由比特股衍生出的比特资产，必须针对一个有效的买单和与交易金额等值的交易后抵押创建。如果买单出价被接受，则抵押品和购买价格则被网络锁定，直到比特美元被回购。块链将把抵押品的红利转划给所有比特美元的持有者。比特美元是完全可替代的，并且所有用于支撑比特美元的比特股产生的红利被汇集，以确定付给比特美元的持有者。

用于支撑比特美元的比特股可能以两种方式被使用：

1、作为比特美元交易中的购买款项被兑付；

2、当支撑比特美元的比特股价值少于比特美元价值的150%时，矿工将使用其发起强制平仓。

当矿工在创建区块时发起强制平仓时，它使用来用作支撑的比特股去购回比特美元并兑付，兑付之后这部分比特美元就不存在了，剩余的抵押品将被发送至空头的地址（并非由矿工保留）。

当矿工被迫发起强制平仓时，网络将收取5%的交易费用以激励市场参与各方积极主动地管理他们的保证金，如果市场变化过快导致了保证金不足，则如果比特美元的需求相对于卖方供应不足，比特美元的市场价格会短时间跌至平价之下。

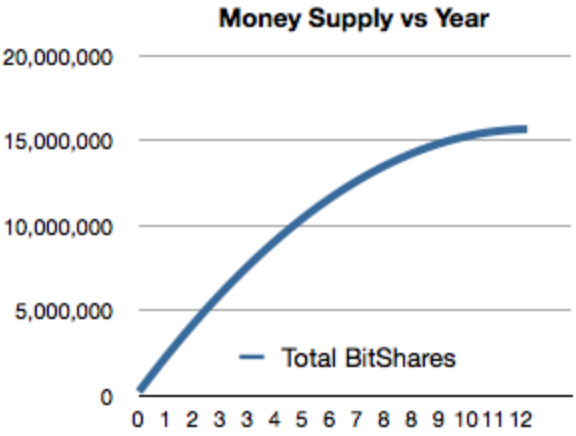
高级交易和合约

由比特股及自动强制平仓组成的基础架构，意味着类似认购和认沽期权之类的合约都能够被创建和交易，这些合约的推销和广告可以离链进行，一旦交易意向达成，可通过相对简单的挂单脚本规则在链上执行。

比特股红利

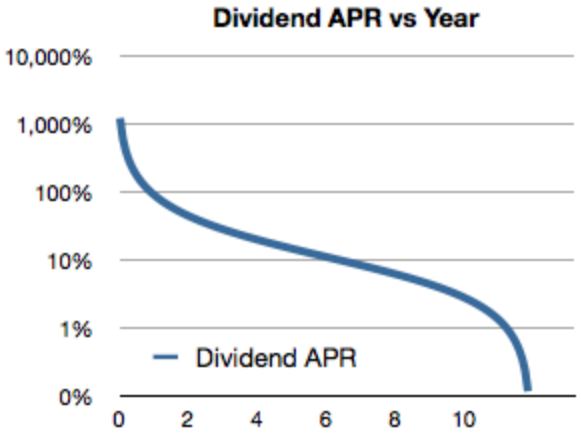
所有挖矿奖励和交易费用的一半将按照持有比特股数占现存比特股总数的比例分配给持有者，比特股总数会按一个不断降低的增长率增长，由每分钟50个开始，直至12年后降低为零，这意味着红利开始也会很高，最后趋近与一个与交易费用成正比的数字。

比特股选择采用12年的发行期，而不是像比特币128年，因为一种货币的正当的功能并不需要通胀，而且在12年中，对块链空间（为满足去中心化和可扩展原则而被限制）的竞争会驱动交易费用/交易量达到一个让矿工有利可图，并且符合市场要求的安全级别的水平。



网络还有其他的手段来生成费用激励矿工：闲置税，平仓费，和‘红利灰尘’。比特币遭受了与所需要的安全级别完全不成比例的挖矿奖励定价带来的麻烦。

完全基于的挖矿奖励和忽略所有的手续费，有效的年红利率按月显示在右图。你会注意到早期的矿工通过采矿和持有获得了很多收益。这将创造市场需求推动早期比特股的净现值远高于后期的比特股并将继续推高价格直到价格稳定。请注意，那些持有比特美元的用户将会获得超过2倍的收益率，因此有机会在新块链的前10年，年利率超过20%。



由于比特美元的红利如此高，它会以比实际美元高很多的溢价进行交易。这个溢价将会是市场基于觉察到的风险和卖空/赎回的相对需求比特美元有效年收益的手段，但是从投资的角度来看，如果美元相对比特股的价格翻倍，那比特美元的价格也会翻倍，这意味着尽管溢价可能有波动，但是不会有汇率风险。

红利结构是零和的，对矿工的奖励是通过“通胀”取自于所有的比特股持有者的，持有者获得的红利同样来自此红利，一个类比是一个每10分钟按1到1.0000001的比例作拆股的股票。结果是，这样的红利确实没有传递新的“购买力”给持有者，因为持有者获得的红利只有通过“通胀”奖励挖矿的比特股的一半。

结果，源自通胀（或者说再分配）的红利导致比特股的持有者感受到的通胀率比比特币的持有者感受到的低50%，最初的红利主要来自通胀，而最后红利则表现为完全来自交易费用的无通胀收益。

红利之所以必须还有另外的几个原因：

1、它们创造了持有空头仓位的机会成本（鼓励补仓）；

2、它们创造了对持有而非卖出的激励（增加了持有的价值）；

3、它们补贴了多头，为其承担的风险；

4、它们把比特股变成了有现金流收入的资产，使比价和变现成为可能；

5、它们使得比特美元，比特黄金能够吸引任何寻求免于汇率风险的投资回报的人买入，使其有了流行的可能。

比特股和比特币的小数点位置/可分割性比较

1个比特币传统上定义为1亿聪，结果我们开始看到有些东西标价为0.0001BTC或者更少。随着比特币升值，价格的小数点后被加上了越来越多的0前缀。这个既让用户难于理解和比较价格，又使得标记一个很小的价格需要一大串数字。此外，人们不熟悉使用毫，微或者纳等小数单位，而习惯使用千，万，亿之类的单位。这些大的单位似乎更加容易谈论、圆整，感知和比较。

在本文中，我们提到的1比特股时，仿佛1比特股在所有比特股供应中占的比例与1比特币在所有比特币供应中占的比例相仿。事实是，采矿奖励会是500万比特股，0.001个比特股不会比一聪更可以分割。用户开始会用百万比特股给物品标价，随着时间的推移会下降到千，甚至到百个比特股。随着比特股网络中使用的小数点的移动，比特股的有效供应会超过15万亿，如果0.001比特股相当于0.01美元的话，可以支持总量超过150万亿美元的现金流。，美国货币供应量（M2）大约是 10万亿美元，这意味着在1比特股相当于10美元的情况下，比特股可以支持大约15倍目前世界经济规模的经济体。

扩展

块链有一个基本速率限制，使得交易可以在工作量证明和网络延迟的基础上被证实和确认，对块链性能的提升到了一定程度之后就需要高端的计算机，硬盘和网络，最终就开始让网络中心化。为了满足去中心化的要求比特股块链将被限制未交易挂单的总金额，并且限制每个链最多支持32种资产。

每个这样的块链被称为比特股交易所（BitShares Exchange，BSEx）。而块链的总体被称为比特股自由市场系统（BitShares Free Market System，BSFMS）。BSFMS被设计作为独立竞争/自由合作的市场实体成长，并不断建立新的与比特股兼容的BSEx，将会因满足市场需求而获益。四个这样的BSEx组成了图示的BSFMS。每个BSEx最多可有32个加密货币—加上本地和全局的比特股货币。每个BSEx有自己的块链来支持加密货币并以本地比特股货币来命名（以红，绿，蓝比特股表示），这些本地比特股可以在本地与构成货币BSEx本地标准的全局比特股（黄色）交易。

BitShares货币交易所（**BitShares Currency Exchange**，**BSCurEx**）和三种潜在的**BSEX**链

不像比特币，比特股可以扩大范围和支持多个完全独立和并行的块。因为每个块链可以交易捆绑在其它块链上的比特资产衍生品，块链之间的价值移动是很容易的。某些用户可以加入两个块链做套利。平行块链结构的结果就是比特股可以扩展到任何容量而不需要普通电脑处理有交易

需求的1-2个块链之外的块链。系统原生支持的全新的“合并挖矿”技术可以确保矿工有效地选择同时进行挖矿的块链，而不允许空闲算力去承担超过实际需要的工作量证明，一次性挖掘上百条块链，而导致网络负担。

某些希望一次性移动数十亿美元的大玩家可以在大型数据中心合并所有的块链，并且在链和链之间的套利。这些玩家不会造成系统的中心化，因为他们并不是必需的。相反，这些大型玩家仅仅会让某些单独的链更加稳定。

公平的合并采矿

合并采矿是许多不同块链可扩展性的关键方面。不幸的是，合并采矿需要Merkle树（Merkle Hash Tree，常用来在分布式计算中保持各节点同步更新的算法）来作为工作量证明，从而需要在块头占用更多的空间在一年以上。如果我们需要建立一个像比特股这样的最终会拥有超过1000个以上的链且每个链上都有一系列的比特资产子集的系统，那么合并采矿就是至关重要的。然而，你并不希望人为的限制Merkle树的深度，也不允许合并的矿工不顾每条链的潜在价值，通过把暴露的每条链都包含在自己的Merkle树中来损害它人获得免费的午餐。

比特股采用了一种新方式来支持合并采矿，通过适当的利润激励来最大限度缩小Merkel的工作量证明分支而不是限制它的大小。假如现在有两个比特股链（红色和蓝色），每个链有不同的资产子集，那么做合并采矿的矿工有三个选择，挖红链、挖蓝链或者合并采矿。如果他选择合并采矿，那么红色和蓝色的网络将会产生接受更大的工作量证明的成本，而矿工的付出将会加倍，所以新的方式可以使用Merkle分支深度来获得工作量证明，如此流向矿工的奖励将会打折扣以与流向红利的部分平衡，矿工的奖励公式为 blockreward / 2^(merkelbranchdepth)。最终的结果就是，如果红色和蓝色的比特股有相同的市场价值和难度的话，那么合并采矿的利润和单个一样。包括红色和蓝色都从增加的哈希能力获益，而矿工不会获得任何额外的价值，除非他希望有新的“可变链”随着时间的推移来增加价值。

如果红色和蓝色链有不同的价值和难度，那么矿工必须基于他们对两条链相对哈希能力分配的增长预期，小心的选择他们要采矿的链。这可以在不强加无利可图的合并采矿于一个大型网络或者创造一个“主/从”链设置的情况下，使良好的和有用的合并挖矿成为可能。

原子化跨链交易

原子化跨链交易问题是指当（至少）两个交易方，爱丽丝和鲍勃，拥有各自的加密货币（如比特币和莱特币 ）并且想在不必须信任第三方（中心化交易所）的情况下交换。

一个非原子化的平凡解决方案是让爱丽丝先发送她的比特币给鲍勃，然后让鲍勃发送莱特币给爱丽丝 – 但鲍勃可以在收到比特币后选择违约，使爱丽丝损失发送的比特币。

进行原子化跨链交易的算法已在比特币wiki中描述，比特股将支持此算法，这将使用户能够在无需中介代理或者信任的情况下交易BitBTC和真实的比特币，整个过程都能被软件自动执行。

这个特性可以用来在两个并行的比特股链之间交易，增加网络的可扩展性。

轮转块链

比特股块链的另外一个方面，是所有尚未匹配的输出挂单不能存在超过1年的时间。超过1年的未匹配的输出挂单将被罚没红利，并且会被在块链中前移并征收5%的交易费。低于平均交易手续费的余额将被全部罚没。这将使网络能够从丢失的密钥中恢复价值并且消除以不断增加的成本（且无收益如果密钥丢失的话）永久存储交易和挂单数据的需求。

因为块链轮转，所以定义处理块链需要的最大磁盘容量是可能的。将来最大容量可以向上调整，但是建议网络基于新计算机中的RAM的平均容量来设置限制。这将确保所有的数据集可以很容易的放在RAM当中，这样所有节点可以很有效的处理所有的交易，这在需要做额外的工作来执行做市商功能的时候是非常重要的。

广义实物传递中介

当与不受信任的有违约可能的“匿名”个人交易时，中介就会变得非常重要。传统的方法是使用能够撤回交易和决断纠纷的中介代理（例如Paypal）。但不幸的是，传统的中介代理必须是在每一笔交易中受到信任的第三方。如果这个中介不是匿名的，那么他们有可能在处理某些交易时承担法律责任，如果他们是匿名的，那该如何被信任呢？

出于法律的原因，对于任何一方，包括中介代理，有义务遵守任何具有法律约束力的合同是非常重要的。这样的合同有可能引发交易对手风险，并且触及与中介和仲裁服务关联的许多法律法规。相反，比特股的中介系统运行的假设是，在任何时候任何一方都没有法律义务来采取任何特定行动，而所有交易方都会在市场力量的驱使下采取诚实和道德的行动。

比特股通过在块链中内置的中介代理功能来解决这个问题。任何用户都可以作为匿名中介代理在块链中注册并定义中介交易所需要的参数，包括：时间表，手续费，诚信保证金，所需证据，在发生争论时需要匿名沟通时使用的BitMessage地址，和其他相关的中介代理推荐的相关流程。某些参数是块链强制要求的（如手续费，诚信保证金和时间表），所有其它的则不是强制要求的，取决于各方自己的意愿。幸运的是，在确保诚信方面，利润驱动被证明是比法律或者法院判决更加有效。

如果一切进行顺利，则中介代理不会介入。然而，如果在交易中出现纠纷，任何一方都可以在块链发起一个新交易来“冻结资金”直到中介代理做出裁决为止。中介代理只有在交易双方划分资金的权力。中介代理也会绑定其他代理。因此，任何一方只要愿意付费，可以对中介代理的做出的裁定反复提出争议，直到连续三次受到同样的裁决为止。

如果某个中介代理有尚未解决的争议，那么任何以涉及此代理的新的交易都不能进入网络。这就会通过在财务上激励中介代理能够诚实且高效的解决所有争议。

所有各方将因为诚实而获利，因为不诚实将遭受损失，企图串谋是不会成功的，因为存在申诉流程并且交易双方可以一起选择中介代理。中介代理将从每次交易中根据他们的服务收取手续费，因此也不会希望冒着损失名誉和保证金的风险来帮助一方而欺骗另一方。

尽管这种中介代理系统在个人之间提供相对快和安全的电汇或者银行内转账，但是它在防止扣款/回转方面的功能有限。有鉴于此，建议所有的付款通过电汇或者ACH（Automatic Clearing House），这样这些支付将被允许在发布给中介代理前过期。

去中心化

去中心化的哈希功能

比特币的工作量证明使用双倍SHA256算法，导致了专门执行此种功能的专用ASIC芯片的生产。这种专业化程度已经使挖矿变成比特币社区中一小部分人控制的高风险的专门业务。这种中心化已经成为网络的包袱，因为矿机有可能像交易所一样被人为操纵或关闭。矿池是集中算力的另外一种形式的中心化。拿掉一个矿池就有可能破坏整个网络的哈希计算能力，可能让交易延迟数天直到难度被调整。

保持工作量证明的去中心化程度的第一步是设计一个能够在CPU这种“通用设备”上最好地运行的哈希功能，它根本不能从专门的GPU甚至是更加专业化的ASIC获益。设计这种算法中有好几个关键点。

首先，它必须基于以最有效的方式尽量多地使用消费者最广泛使用的晶体管。RAM和缓存使用非常密集，高优化的ASIC也已经分布甚广。历史上，RAM和CPU算力增加的速度基本一样，因此，使用RAM，将会让专门的ASIC芯片甚至GPU芯片不能通过“并行”的方式来优化。这自然让所有的性能都是串行的。使用RAM的另外一个特性就是，当大多数时间，CPU在缺乏数据时，系统总线的速度要比CPU的能力重要的多。如果通过优化CPU的处理速度是无法解决CPU缺乏数据的瓶颈，因此即使提高10倍计算能力也不会提高数据通过的能力。

其次，它必须基于不带分支预测的连续数据处理。仅此一点就能阻止绝大多数的并行数据或者预取优化的操作，因为GPU的架构在这方面比CPU差远了。GPU还同样受困与内存总线的限制，如果不能保持每个GPU核心有着足够小的本地缓存，那么它的表现会显著下降。这些特性可以让CPU能力能够分布开，并且阻止某些专门设计的有着巨大优势硬件的攻击。

建议工作量证明使用SHA256为广泛存在于128MB RAM中的8位快速随机数生成器提供种子。在填充RAM的过程中伪随机分支会阻止传递并导致某些额外的CityHashCRC128操作混入伪随机填充到整个128MB地址空间当中。当所有的128MB都被填充完，通过CityHashCRC128来计算哈希，最后使用CityHashCRC32的SHA1获得结果。

这些建议的操作是充分利用下面CPU相对于GPU的优势特性，来确保CPU才是最理想的ASIC。

1、GPU在单线程情况下每4个时钟周期只能执行1个指令；

2、CPU的工作频率大约是GPU的3到4倍；

3、CityHash利用类似Intel酷睿i7的超标量体系 CPU可以在每个时间周期中执行多个指令；

4、CityHashCRC128利用硬件加速CRC32指令，这需要处理器支持SSE4.2指令集，而目前SSE4.2不存在于GPU中，未来加入的可能也不大；

5、在出现分支误预测时，GPU的表现非常糟糕。

根据因素1、2和3，CPU在单线程模式下的处理速度大概是GPU的32到64倍。而由于CRC32

的因素导致的软件层面上的另外4倍速度的提升，总共CPU在单线程模式下处理速度会是GPU速度的128到256倍。最后，分支误预测会加剧GPU的劣势。总的来说，我们预计一个GPU大约需要2048个完整多处理器（不是流处理器）和大约256GB的RAM才能在这一特定问题上和一个4GHz的Intel酷睿i7的处理能力相当。我们把数字定在必须大于64，以使足够低的内存就可以应付最高端的GPU。

因为工作量证明比签名验证更加消耗CPU算力，一个辅助的花费1秒的工作量证明将被执行并在块头工作量证明被验证和被节点广播之前被一个单独的SHA256操作验证。这将防止对网络的拒绝服务攻击。

最后一个去中心化的保障，就是有可能通过网络升级哈希算法以保持其针对CPU优化的能力。一旦明显察觉非商业化的硬件能够在采矿时拥有很强的优势，那么在这种优势被实现前，网络可以升级哈希算法。这方面的微小威胁以及在发布块链时对执行此种计划的意图的声明将阻止玩家在有特殊目的硬件上做重大投资，并且使他们在这类投资贬值时所做的任何不正当竞争指责无效。

内置的去中心化矿池（**P2Pool**）

P2Pool采用的技术，将可以建立一个没有中央服务器的分布式矿池，可以让大多数用户即使在难度增加的情况下快速便捷的进行采矿。这将不会是比特股协议要求的，但是会有网络支持。

安全

51%的拒绝服务攻击

由于所有的节点受到红利这样的财务激励，他们会积极主动地拒绝那些没有包含80%已知正确交易的新块。所有节点都有财务激励去验证块链，并拒绝和那些创建使他们失去红利的新块的用户共事。所有的矿工都被激励去拒绝那些包含大量“前所未见”交易和费用的块，因为这意味着有人在造假以骗取手续费或操纵网络。因为绝大多数用户都是因为“有利可图”才进行采矿，他们会积极主动地合作来阻止这种操纵企图。于是，要进行51%的DOS攻需要耗费攻击者巨额成本来收买整个网络，而他们的对手的挖矿收益将会提高，会使51%双重支付攻击变得更加昂贵。

加密通讯

所有节点之间的通讯都因为两个原因而被加密：它可以阻止通讯包过滤，并使确定新交易的来源变得更难。

比特股经济学

比特股试图让所有的参与者积极活动以确保即使是在极端动荡的市场中抵押要求也可以被满足。为了说明市场中力量是如何与比特股的块链规则互动的我们考虑几个市场场景。

比特股价值的快速下跌

如果比特股的价值相对于比特黄金快速下跌，那么系统所有的空头必须面对“逼空”，强迫他们在爆仓前积极行动。如果跌至他们的红线，他们将会支付5%的手续费或者更糟，损失全部的抵押品。逼空的结果就是比特黄金会急速上升超过市场上的黄金价格，使更多的空头面临爆仓。这会为新的空头创造机会进入市场通过全额抵押卖空建仓。这些新的空头将会在逼空结束之后的价格回落中获利。因此市场的所有参与者会积极的监视价格和他们的抵押品，从而减少市场的波动。

比特股快速升值

如果比特股的价格相对黄金快速升高，那么比特黄金持有者将会看到比特黄金相对比特股被高估。了解到其他市场的参与者会试图基于相对黄金的价格进行买或者卖比特黄金，比特股市场会出现大量的比特黄金抛盘，直到比特黄金的比特股价格跌至黄金的比特股的价格。

比特黄金价格的跌落就意味着空头会超额抵押从而引发不必要的机会成本。这会驱使他们平仓获利了结。

连接黄金和比特黄金的价格

如果能形成一个共识，认为比特黄金就是由当前红利率下的1盎司黄金债券的衍生品，那么所有的市场参与者都将获利。然而，市场不会一开始就‘信任’比特黄金。结果是所有的市场参与者最初挂单的价格会很散。当市场深度增加价格范围会缩小直到一个市场共识价格形成，该价格会接近当前红利率下的1盎司黄金债券的价格。

交易各方会根据他们判断的比特黄金的价格走向决定做多还是做空。唯一理性的投资办法就是假设它会跟随实物黄金的价格，因为有什么理由认为它会在某一特定方向偏离实物黄金的价格呢？唯一的价格偏离的理由就是比特黄金的供需变化使得它相对实物黄金的价值提升或打折，这样的提升或打折幅度将会基本上是固定的并且不受比特股与实物黄金之间的汇率风险影响。

在ETF黄金和实物黄金价格之间有很明显的差别。因为大多数个人不能直接交易ETF黄金，但是可以交易金币。比特黄金可以定义为一盎司鹰扬金币（美国造币局标准1盎司金币）的现货价格。这样和ETF价格的人为操纵有轻微的脱钩，而且为鹰扬金币加上了溢价。

如果没有人竞标比特资产会发生什么？

首先必须理解的是，比特资产的价值总是和支撑它的红利价值成正比，因此，空头仓位将一直产生机会成本，同样，多头将一直有不依赖于比特股价值的收入流，这种高于市场水平的红利率将吸引新的买家买入比特资产，也就是说，比特资产总是有基于其相对红利率的流动性，因此只要有人竞标比特股，就会有人竞标比特资产。

因此，首先买入比特黄金的早期用户将面对有限的风险（如果有的话）。如果比特股的年红利率是10%，那么当交易成比特黄金之后，用户将获得双倍的收益，即便他们是仅有的买家。当需要“松开”这个交易的时候，价格将决定于更急需流动性的一方，如果空头急于停止付出让人泣血的机会成本，他们将被迫在更高的价位买入。如果多头需要将比特黄金转换为另外的资产，他们会选择低价出售。无论怎样，在任何比特资产市场中都不会只有两个只关注获取更高收益率的玩家。

红利的市场效应

比特美元和比特股都按一定的利率支付红利，红利支付比例通常在1.5到2.5之间(因为比特资产的抵押比例通常是1.5-2.5)。定价时必须计算两边的与比特美元和比特股成比例的收入流的净现值，这样比特美元相对比特股的价格将几乎100%与美元和无红利的比特股的汇率相关。最终，比特美元相对于美元的溢价或折扣将由空头的“借入机会成本”和多头要求的“风险溢价”共同决定。所有其它的比特美元持有者获得的回报将出自其所属的比特股网络的整体升值。

如果市场崩盘导致保证金不足将会发生什么？

这种情况下空头账户将会被按市价清算，短期内多头仓位价值将会降至市场平价之下。只有最严重的比特股价值的崩溃才会触发这样的事件，因为不大可能在60分钟内发生所有其它资产类型相对于价值稳定的比特股的升值。当价格低于市场平价时，市场参与者有两种选择，持有直到市场稳定，或者在市场调整期割肉，因为所有市场参与者都知道比特美元的价格必将因为市场力量而恢复，任何有割肉盘出现的时候都会有很多买家进场建仓从而为价格提供支撑。

只有当整个系统崩溃，比特股才会变得毫无价值而每个人都会受损，这是非常低概率的事件，除非块链算法或者加密机制被破坏。早期的使用者将因为货币总量尚小而有更高的收益率，这是对他们甘冒巨大风险的补偿。后来的使用者会对算法更有信心因而他们的收益率会低一些。

如何为比特美元定价

到此，我们已经展示了比特美元是如何和美元高度关联的；然而，我们还没有提供一个合理的方法来真正确立这个价格。现在让我们看一下拥有比特美元的投资建议。你将获得一种匿名的，

安全的，付息的资产，它有比特币的所有特性，却没有任何比特股/美元的汇率风险，因为20%的年收益率你必须将其和其它的美元投资，例如3%年息的的银行存款比较。在进行了净现值计算后，你可以确定仅基于产生的收益1比特美元就大约应该卖1.14美元。

这个数值应根据加密货币特性带来的溢价和风险折扣而调整，并导致比特美元的价格在1.10美元到1.20美元间波动，这个价格区间将随着能感知到的风险不断降低和收益不断清晰而日以收缩。

至此我们仅讨论了买方的定价公式，但在任何人能拥有比特美元之前必须有人先创造它，这意味着必须有人放弃10%的年收益而建立空头仓位。该空头需要美元相对比特股跌价10%以保本，如此他只有在1.14美元的价格之上卖空才能获得足以覆盖成本的收益（10%）。这会导致比特美元的供应增加直到价格稳定在1.14美元左右。如果他预期比特股将升值超过10%，他将通过在1.14美元的价格下卖空以吸引更多买家，从而有效地扩大空头仓位。

能够在1.14美元的价位之下购买比特美元意味着实际年收益率提升到了20%之上，必须为比特美元支付高于1.14美元的溢价，意味着实际年收益降低到了20%之下。最终，市场将基于平衡出借美元给网络的风险/收益率所需的利率为由比特股支撑的比特美元建立正确溢价。

提示：以上例子中的价格都基于假设的净现值中包含的3%的贴现率，并且只能代表评估公平市场价格的一种方法。最终所有的价格都会在市场中被远多于提及到的因素决定。需要理解的关键一点是，比特美元是一种能够让比特股头寸对冲比特股/美元汇率波动的资产并且不应该被期望与美元拥有精确的*1:1*的汇率。

启用本地交易所交易比特美元的意义

LocalBitcoins（一个比特币兑换网站）用户面临的挑战是，任何一个指定城市的买卖价差都比全球市场的买卖价差大得多，结果是在狭小的本地市场交易成本要大得多，而且，没有使精准交易成为可能的全球化中心市场，价格发现将变得更难，而这又进一步扩大了买卖价差。

由于比特美元采用全球化的去中心化方式交易，并且保持近似于美元有息债券的价格，比特美元和美元现钞之间的买卖价差会比LocalBitcoins上的价差小得多。这种减小的价差的影响是，它有可能会和中介费用和远程交易所的时间延迟竞争，因此将会出现更大的本地交易所。

这还意味着你的朋友和家人可能愿意借给你美元现钞来获得比特美元，因为他们不必担心汇率风险并且能从中获得真实的回报。一旦他们开始获利，恐怕他们就再也不会停下来了。

案例

本地存款

奶奶想从她的美元获得10%的回报，但是她不会使用计算机。于是她的孙子决定来帮助她，他把美元从奶奶那里拿来购买BitUSD。他通过在分类广告网站上发帖说他寻求买入一些BitUSD。某人回应他说他可以和他用纸币来交换BitUSD。交易完成后，孙子就可以打印出私钥并且给了他奶奶，让她放在床垫下。

本地提现

一年后奶奶决定拿回她的美元，于是联系了她孙子并且把私钥给他。于是孙子在分类广告上找寻需要买BitUSD的人。他们会面并交易成功后，孙子把美元交给奶奶。

中介远程存款

乔治住在一个偏远的地方，离他最近持有比特美元的人也在个小时的路程之外，幸运的是，他有家人住在大城市，所以他打电话给他哥哥表示愿意支付10美元报酬帮他从当地购买价值1000美元的比特美元。他哥哥同意后，乔治打过来1010美元，他哥哥买了1000比特美元后，（通过比特股块链）把比特美元发送给乔治。

卖空

山姆是一个专业加密货币的交易者。他一直密切关注市场，他发现比特美元相对比特股高估。于是决定抛售比特美元来“做空”。这样他就必须放弃红利。如果他是对的，比特美元的价格（相对于比特股）就会下跌，那么他就可以以更低的价格买回比特美元，且获利将会超过他的红利。如果他是错误的，那么比特美元的价格会上涨，网络强行平仓让他遭受损失。所以，如果你想卖空获利，你最好期望价格下降的幅度超过你放弃的红利，或者你可以以一定的溢价来售出比特美元。

杠杆投机者

亚历克斯一个比特股（BTS）的早期进入者，他已经挖了100个BTS，并且相信它们会在几个月里增值3倍。他可以简单的持有，但是他希望通过杠杆升值。于是，Alex就卖空比特美元。如果他是对的，那么他就会从卖空中获得比简单持有BTS更多的红利。这样，亚历克斯在比特股已经快

速升值且支付高红利的早期为了规避风险而创建了比特美元。

货币对冲交易者

爱丽丝是一个从事美元/欧元市场的货币交易者。爱丽丝挖了一些比特股，并且用它们来购买比特欧元（BitEUR）和做空比特美元因为她预期欧元会相对美元升值。当她保持这样的仓位，对于比特股的价格变化她没有风险净敞口，因为任何空头仓位的损失都会在多头仓位获得补偿。

比特股泡沫投机

大卫认为比特股的价位已经出现泡沫，所以他买进比特美元来期望相对于比特股升值，同时也希望在过程中收获高红利。

商户服务

费尔南多正在运营一家在线商店，希望通过加密货币接受付款。不幸的是，所有他的供应商价格都使用美元。费尔南多于是选择使用比特美元来标价。这样的结果是他的客户获得了稳定的价格，费尔南多避免了使用类似于Mt.Gox之类交易所产生的交易费，而费尔南多还能在等待结算的时候获得红利。

比特币投机者

卢克有一些比特币，它希望使用比特股来买一些加密比特币（BitBTC）。首先，他必须找到一些BitBTC，于是他找到拥有一些BitBTC并且想换成真实BTC的查尔斯。于是，卢克和查尔斯使用跨链交易来交换BitBTC和BTC，不太需要担心'汇率'，它们应该是1:1。

跨链交易的功能将会内置在比特股客户端，卢克和查尔斯只需要指定各自的地址和交换比率即可。客户端将会支持广播出价来"实时"和对手协商，所有的交易会在20分钟内"过期"。因为BTC对BitBTC是非常小的市场，所以应该有很快的流动性，可以让所有节点都是激活和互动状态，而不需要担心市场太单薄。即使同时在线的只有2个人也能正常工作。

100%准备金的黄金银行

在创建可以支付红利的比特黄金时有个有趣的副产品，它将建立某种去中心化的，点对点的，"100%储备金的黄金银行"，如果某人想要在这个银行存入，需要发布广告表示想用1个金币来换取一个1比特黄金。而某个想要从这个银行提取黄金的人将会回应这个广告。假设那些储户和提款的人的资金是1:1的话，这就应该几乎没有任何溢价或者交易手续费。

如果储户比提款者多，那么储户就必须支付一小笔“ATM”手续费进行存款。如果情况相反，那么提款者则不得不支付“ATM”手续费了。“ATM”手续费将会成为那些储户和提款者的供需调节器。当存款费用搞，储户就会持有直到它下降。高存款费用将会刺激空头来借更多的比特黄金卖出以获得实物黄金，来从手续费中获得利润。当提款费用上涨，就会吸引那些将之理解为存款有补贴的储户。

注意：称呼系统为“银行”仅仅是为了促进理解的一种比喻。比特股不是银行，也不吸收任何存款，也不承诺支付任何费用。很明显，真正的一个100%储备金的黄金银行一定会收取你的保存和交易费用，并且需要一定周期的定期存单来提供回报的。

比特股和比特股衍生的比特资产的法律分类

在提供我们关于法律方面的意见前，我们必须提醒阅读者，我们不是律师，并且下列陈述也不构成专业法律建议。在根据我们下面表达的意见而采取任何行动前，请根据你的情况咨询法律专业人士。

纵观全文，我们参照了买多，卖空，保证金，认购认沽期权和其他传统的金融术语和工具，然而这些都是用来解释关于全新的比特资产表现的类比。我们认为，除了最为常用的术语“资产”之外，这些工具不符合关于金融资产，工具，债券或其它任何书面术语的法律定义。在尝试分类这些新的比特资产前让我们回顾一下现在的定义。

金融资产是因合约要求而衍生出价值的无形资产。

金融工具被定义为“形成—个实体的金融资产并形成另—个实体的金融负债或权益工具的合同。”根据国际会计准则32号和39号。

合同是由两个或两个以上交易方的自愿协议，每一方都有意愿在他们之间创建一项或者多项法律义务。合同是保证某事会发生或不会发生的有法律强制力的许诺。

一份合同的元素包括：

1. 提议与接收，意见的一致。

2、由法律约束的意图。

3、应考虑的因素。

此外合同的各方必须具备履行合同的能力，其目的必须是合法的，形式也必须是合法的，目的必须是建立一个法律关系，各方必须都同意。

根据欧盟法律，你必须考虑MIFID（金融工具市场指令）。该指令把一个规范的市场定义为被一个市场运营者运营和/或管理的多边系统，它把多个通过金融工具交易的第三方聚合在一起 - 在系统中根据非自由裁量规则 – 用一种产生一个承诺在其规则和/或系统下交易的金融工具合同的方式。这些第三方被授权并根据条款三依法运作。

所有现有的金融资产和负债（包括现金）背后共同点就是合同义务。如果没有一方向另一方做出的合同责任，那么按照定义比特股衍生的比特资产就不是金融工具。那么让我们看一下，我们能否能从比特股那里找到满足所有的，或者是大部分合同要求的特性。

1）录入买卖交易到块链

买入或者卖出挂单是由单一匿名的某方发出的加密签名交易。这里没有其他方的签名和应尽的法律义务。买入或者卖出挂单不具有法律地位，也没有创建法律关系。这些挂单被没有能力与提交买卖挂单的匿名方订立合同的匿名个人组成的网络处理。理论上，买入挂单包含了对把挂单写入区块的人的支付，并且可以视作被矿工签名和接受。然而，当交易被包含在块中，匿名的双方依然没有明确的义务或者法律关系。更进一步说，被一个矿工简单的把交易包含到一个块中并不会真的导致交易的执行。必须是被所有网络中其他节点都接受。即便如此，在双方之间还是不存在法律关系和义务。甚至，被接受的交易的结果仅仅是对全局共享数据库的匿名更新，等同于自由言论。

2）卖空交易录入到块链

这类交易具有所有买入/卖出交易的特性，唯一的不同是交易中输入的比特资产类型，以及输出的性质。它依然是被单个匿名交易方签名并永不会被其它交易方签名，这里并没有被创建的法律义务或者两方或多方间的法律关系。

3）矿工执行的保证金追加和平仓

没有哪一方有合同义务追加保证金或者强制平仓，然而，当网络多数同意时，没有哪一方有能力阻止他们的仓位被轧平，结果是，任何一方都没有追加保证金的义务，也没有法律上不追加时需要承担的强制性后果。事实上，没有什么市场实体能强制追加保证金，因此没有谁需要对未能行动负责。

4）开发者和用户之间的合同

比特股是一个能够被用来在任何数量的个人间交信息的协议，开发者发布软件开源代码，但并不确保或承诺有任何特殊表现。软件用户选择使用的软件版本和加入的网络，因而能够完全控制如何应对他们从网络获得的信息。用户甚至可以自由地去按自己的愿意修改软件，因而软件的表现和决定是用户，而不是开发者的意愿的延伸。

最后，比特股的开发者只是创建了一个管理去中心化数据库的财务系统，数据库的任何输入都不在开发者的控制之下。

5）交易所监管

一个由市场运营者运营的中心化比特币/莱特币交易所可以被监管，因为接受的加密货币存款都被转换成特定服务器上以账户余额形式存在的金融工具兑付承诺。

而在比特股这里不存在市场运营者，也没有任何一方在任何点上，出于把连接多个第三方的目的把比特资产转换成金融票据。原因是这里没有甲方乙方或者各方之间的合同。

6）分布式中介和仲裁系统

为促进传统资产和金融工具的交换，比特股提供了分布式的，非正式的，非捆绑的中介和仲裁系统。每一个无争议的中介交易都有两个交易方而当争议产生时就会有三个交易方。交易双方订有无约束力的协议，其中包含了仲裁条款，允许预先设定的，但是匿名的第三方根据他们自己的判断以完全无约束力（法律意义上）的方式进行裁定。在两个交易方之间存在部位其它网络成员所知的私下非正式协议。中介代理不能接收资金也没有把资金发送给交易两方之外的第三方的能力。

中介代理会遵从任何法律，规章和仲裁执照要求，如果用户希望他们的裁定有法律强制力的话。幸运的是，中介代理和用户明确任何一方都没有法定义务去执行特定行为，因而没有意愿去创建法律关系。通过特别声明，在任何时间都没有哪一方有法律责任去遵从任何特别条款，就会消除建立法律关系的意愿，结果是所有各方都以一种非正式的，完全自愿的方式活动，远离法庭判决。就像同意在酒吧会见某人而未能到场一样。

社会和市场压力会促成所有各方在法律义务完全缺失的情况下作出诚实的和道德的决定。

唯一遗留的法律问题是一个从事比特资产和有形货物或传统金融资产（如现金）间交易的个人是否会被理智的监管系统或法庭归类为货币转移者，FinCIN已经发布指引表示用比特资产买卖非金融资产不被视为从事货币转移或货币服务业务，只要只存在两个交易方，没有合同，并且没有哪一方是在代表第三方交易，就不存在货币转移。这就好比声称，在分类广告上以非商业的方式用黄金交换现金的某人是货币转移者一样。

由于我们并不是律师，上面所阐述的所有意见并非构成法律建议。所以当你准备采取任何可能产生法律后果的行动前，请寻求专业的法律建议。

替代系统

对于创建交易与其它资产如美元、黄金或白银绑定的数字货币的去中心化交易所已有了许多尝试，比特股是作为这些尝试的替代方案引入的。我们下面会列出已有的尝试中比较成熟的方案，并且讨论它们与比特股之间从标准制订开始就存在的不同点。

Ripple

Ripple是一个点对点的网络，使用自定义的货币（XRP）来方便传输和交易或者以任何单位交换货币。Ripple不是一种无需信任的网络，而是一种可以让朋友或者家人通过网络来转移信用的方式。每个个人必须发布一个把信用扩展到他们认识的每一个人的信用路径，这导致了违约风险。我们认为，这不是一种社会化的可行安排，它意味着大多数人最终要使用Ripple网关。而Ripple的网关就像一个银行，通过在Ripple网络交换信用接受存款。网关可能遭遇货币转移者或任何接受存款的公司遭遇的法律和监管问题，最终结果就是Ripple不是去中心化的，也不为所有各方提供有限责任。

此外，Ripple不支持卖空，期权因此并不多样化。离开了对Mt.Gox和Bitstamp一样的中心化的网关的依赖，货币交易就不是聚合的，原子的或者被动的。

最后，Ripple并不保护隐私，因为每个人必须把他们Ripple的身份和他们真实世界的身份相关联，以建立和朋友，家人和网关的信用路径。Ripple目前是不开源的，尽管它承诺以后会开源。

最后，Ripple提供的商业价值不大，不足以吸引加密货币运动之外的人或者商业机构去开办一个网关。因此难以流行。

LocalBitcoins

LocalBitcoins是一种内置中介服务的场外交易所。虽然交易发生在个人之间，但是网站不是去中心化的，而且中介服务依赖于个人信用。

此外，交易不是迅速、原子化、保护隐私、聚合的，也不安全。价格也不是正确的，因为没有买入卖出系统且所有交易都要最终参照中心化交易所的价格。

它不是多样化的，因为没有卖空，期权等。网站还由于中介服务可能会面临巨大的责任。

彩色币（Colored Coins）

彩色币是一种通过标记块链中的比特币来把它变成一种加密化的不记名债券的方法。系统本质上是基于对发行人的信任，要承担巨大的法律责任，而产生的不记名债券在发行者之间是不可

替换的。这个系统依然没有卖空，期权因而缺乏多样性，也没有解决去中心化挂单列表和被动挂单执行的问题。最后，因为没有价格建议，会难以流行，也难以增加在市场中的流动性。彩色币的交易不是被动的，没有中心化的交易所不能聚集。

Open Transactions

Open Transactions 是一种联合交易服务器系统，允许用户办理、经纪和交易由第三方加密的不记名债券。该系统本质上是基于对发行人的信任，需要审计交易服务器，而且因为不同的美元债券发行人不可互相替代，将导致狭窄市场中的（价格）宽散布现象。创建“一篮子发行人”会分散，但不会消除违约风险，而且等于用高信用发行人的贡献来补贴低信用发行人。系统也未提供有吸引力的特性来促成流行，并且推荐的在多个服务器间协调价格的系统也违法了价格正确原则。

目录

100%准备金的黄金银行

比特股和比特股衍生的比特资产的法律分类

1）录入买卖交易到块链

2）卖空交易录入到块链

3）矿工执行的保证金追加和平仓

4）开发者和用户之间的合同

5）交易所监管

6）分布式中介和仲裁系统

替代系统

Ripple

LocalBitcoins

彩色币（Colored Coins）

Open Transactions