Borderless 无界

区块链去中心化数字资产交易所

注：本白皮书正在积极修订中，非常欢迎来自您的意见。

目录

1. Borderless（无界）的介绍

Borderless（无界），是一个去中心化的多功能数字资产交易系统。这意味着它可以演化成多种不同形态的 Borderless 资产(简称，BDS)。Borderless 的运作方式类似于比特币，但是一些优化和新的规则让 Borderless 的价值更鲜明。在 Borderless，持有 BDS 或者由其衍生资产一定时间的用户，可以获取一定比例的红利收益。这些红利收益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。

2. Borderless 系统的市场机制

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。Borderless 的目的是能够作出市场和自身共同借鉴的基础示范。

1）Borderless 内置去中心矿池

Borderless 采用的技术，是一个没有中心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，也能快速便捷的进行挖矿。这将不是 Borderless 协议中的硬性要求，但是会有回归到网络矿池的数字资产对去中心矿池的支持。

2）系统安全

a） 51%的拒绝服务攻击

所有的见证节点都有财务激励去验证块链，所有的矿工也同时被激励拒绝那些包含大量“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奖励收益才进行挖矿，用户市场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 攻击需要耗费攻击者巨额成本来收买整个网络，而用户们的挖矿收益将会提高，会使 51%双重支付攻击变得更加昂贵。

b） 加密通讯

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

3. Borderless 承兑商

Borderless 承兑商：为用户提供法币与 BdsCNY，BdsUSD 兑换服务的商家。许多承兑商会喜欢一兑一赎回这种低风险的做法，这会让兑换 BdsCNY 出现一些微小的浮动。最终，当用户通过承兑商从 BdsCNY 兑换成人民币时，将会支付一笔少量的手续费。

而另一方面，很多用户都希望直接将 BdsCNY 兑换成法币人民币。在这种操作模式中，承兑商需要提供一个固定百分比金额的交易手续费，以提供所有的承兑服务。承兑商会试图通过提供尽可能低的费率来进行竞争。

4. Borderless 系统的技术支持

1）高效且可扩展性能

Borderless 系统实现超 10 万次/s 批量转账

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，能够为业界提供一个有可能代替现有金融平台的解决方案。为了能够实现比 VISA 和 MasterCard 每秒可以处理交易数量更快的速度，无界从底层开始重新设计。通过股份授权证明机制，无界网络可以在平均一秒的时间内确认超 10 万次转账交易。

Borderless 系统架构总览

要达到行业里面最顶级的性能，无界借鉴 LMAX 交易所的经验。这个 LMAX 交易所可以在每秒内处理高达 6 百万次的交易。无界借鉴其技术的关键点，如下：

a) 将一切东西放在内存里面
b) 将核心的业务逻辑放到一个单线程里面
c) 将加密算法操作(哈希和签名)放在核心业务逻辑以外
d) 将校验的操作分成状态独立和状态依赖检查
e) 使用一种面向对象的数据模型

通过遵守这些简单的规则，无界在未进行颠覆式优化工作的情况下，实现了每秒处理 10 万次转账的高效性能。如果有进一步的优化工作的话，会让无界可以达到与 LMAX 交易所相近的性能表现(即每秒 600 万次)。需要注意到，无界达到这样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，不可能达到同样层级的性能表现。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。 无界的技

术逻辑能够让这个单线程的执行达到极可能的高效。

Borderless 系统核心业务背书

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，从你的银行账户里支取金额。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。

2) 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。

LMAX 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。

3）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。

4）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。

5）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。

6）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。

7）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。

Borderless 无界系统的高效性能的成功创建，是建立在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。这就是无界做的事情。

5. Borderless 系统的块链市场规则

1）块链市场的交易算法规则

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。Borderless 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。

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 交易一样，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。

2）创建 BdsUSD（或 BdsCNY）资产

BdsUSD（或 BdsCNY）资产是一个 Borderless 平台的衍生 Bds 资产，必须针对

一个有效的买单与交易金额等值的交易抵押创建。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 BdsUSD（或 BdsCNY）资产被回购。块链将把抵押品的红利转划给所有 BdsUSD（或 BdsCNY）资产的持有者。BdsUSD（或 BdsCNY）资产是完全可替代的，并且所有用于支撑 BdsUSD（或 BdsCNY）资产的 Borderless 产生的红利被汇集，以确定付给 BdsUSD（或 BdsCNY）资产的持有者。

用于支撑 BdsUSD（或 BdsCNY）**资产的 Borderless 可能以两种方式被使用**

1、作为 BdsUSD（或 BdsCNY）资产交易中的购买款项被兑付;

2、当支撑 BdsUSD（或 BdsCNY）资产的 Borderless 价值少于 BDS 资产价值的 175%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 BDS 去购回 BdsUSD（或 BdsCNY）资产并兑付，兑付之后这部分 BdsUSD（或 BdsCNY）资产就不存在了，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 ,网络将收取一定比例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 BdsUSD（或 BdsCNY）资产的需求相对于卖方供应不足，BdsUSD（或 BdsCNY）资产的市场价格会短时间跌至平价之下。

3）高级交易合约

由 Borderless 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。

6. Borderless 系统的功能特性

1）发行新资产和身份管理

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，Borderless 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。Borderless 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。

Borderless 平台能够提供一种称之为“用户发行资产(user-issuedassets ,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，可以设想某个货币交易所能够利用 Borderless 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，同时将相关的 UIA 凭证存入客户在 Borderless 的白名单账户中。而这些客户能够使用 Borderless 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，Borderless 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 Borderless 完成资金的进出。

企业可以直接在 Borderless 的区块链上发行自己的公司股票，而且这些 BorderlessUIA 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 Borderless 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 Borderless 展示和交易 UIA。

2) 去中心化资产交易平台

Borderless 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 MFGlobal，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 Borderless。

3）去中心化的平台价值

去中心化让 Borderless 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。

4）快，但不会“太”快

随着 Borderless 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。

5）安全

美元，欧元，比特币和黄金，在 Borderless 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 175%以上的准备金的情况下，你可以放心，Borderless 在任何市场中都将具有偿付能力。所有准备金都会以 BDS 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。

6）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 Borderless 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。

7）更低的市场交易手续费

因为每笔交易只少量的手续费，其他交易所会根据你的交易量来收取一定比例的费用。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 Borderless 更加便宜。

8）全资产交易平台

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 Borderless 交易所上几乎没有任何限制。Borderless 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 Borderless 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 Borderless 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

Borderless 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 Borderless。

9) 开放源代码和完全透明

无界源代码已在全球最大第三方开源站点 github.com 公开。整个交流是开源的，由一个非常开放的社区支持。没有任何地方会做到像 Borderless 一样的透明。

10) 隐私

通过使用 Borderless 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。

11) 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。

12) 保证金和卖空

如果你想要一些杠杆来增加你的收益，Borderless 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。

13) 银行业的未来

Borderless 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 Borderless 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 Borderless 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 Borderless 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 BdsUSD，这是数字资产行业中最棒的交易所，也是我们的秘密武器。

14) 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。

a) 收到数字货币来发行 IOU(欠条)
b) 收取法币来发行 IOU
c) 处理订单撮合
d) 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。

15) 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。

16) 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 Borderless 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。

17) 有抵押的区块链 IOU

比特资产(BdsAsset)系统是 Borderless 最核心的部分，它在 Borderless 的系统中

通过建立 300%的抵押来创建。BdsUSD 除了能够拥有 BdsUSD 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 BdsUSD 而获得价值约 1 美元的 BDS。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 BdsUSD，并且返还价值 1 美元的 BDS。

只要 Borderless 它本身在合理的价格波动范围内，那你持有 BdsUSD 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 Borderless 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 Borderless 本身协议和软件出现了问题之外，否则没什么能够影响 BdsUSD 的价格。

当你把你的持股 BdsUSD 的价值将继续只要 Borderless 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。Borderless 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，BdsUSD 是安全的反对几乎一切，但在 Borderless 协议本身就是一个无法修复的软件错误。到时候 Borderless 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 BdsAsset 机制，请参见讨论该机制的详细文章。

18) 全球统一的挂单账本

一旦市场能够接受 BdsUSD 和 BdsBTC，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 BdsUSD 和 BdsBTC 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 BdsUSD 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 Borderless 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。

19) 椭圆曲线密码学

椭圆曲线密码学（ECC,Elliptic curve cryptography）是基于椭圆曲线数学的一种公钥密码的方法。椭圆曲线在密码学中的使用是在 1985 年由 Neal Koblitz 和 Victor Miller 分别独立提出的。

```
int secp256k1_ecdsa_verify(const secp256k1_context_t* ctx, const unsigned char *msg32, const unsigned char *sig, int siglen, const unsigned char *pubkey, int pubkeylen) {
        secp256k1_ge_t q;
        secp256k1_ecdsa_sig_t s;
        secp256k1_scalar_t m;
        int ret = -3;
        DEBUG_CHECK(ctx != NULL);

DEBUG_CHECK(secp256k1_ecmult_context_is_built(&ctx->ecmult_ctx));
        DEBUG_CHECK(msg32 != NULL);
        DEBUG_CHECK(sig != NULL);
        DEBUG_CHECK(pubkey != NULL);

        secp256k1_scalar_set_b32(&m, msg32, NULL);

        if (secp256k1_eckey_pubkey_parse(&q, pubkey, pubkeylen)) {
            if (secp256k1_ecdsa_sig_parse(&s, sig, siglen)) {
                if (secp256k1_ecdsa_sig_verify(&ctx->ecmult_ctx, &s, &q, &m)) {
                    /* success is 1, all other values are fail */
                    ret = 1;
                } else {
                    ret = 0;
                }
            } else {
                ret = -2;
            }
        } else {
            ret = -1;
        }
```

```
        return ret;
    }
```

7. 推荐计划

Borderless 是将会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一定比例的交易手续费。Borderless 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 Borderless ,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一定数量的现金返回，批量折扣，并且那些你带来的用户们，你有机会获得他们一定比例的交易费用。缴纳一定的费用成为 Borderless 终身会员，这会非常容易的进行支付和获益推荐奖励。

工作原理

每一个新的帐户必须由现有的帐户创建 ,之所以有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一定的费用来升级成为一个终身会员。当一个账号成功升级后，缴纳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一定比例的现金返还。

8. 无界与其衍生资产的法律分类

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 BDS 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 BDS 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“形成一个实体的金融资产并形成另一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：

a) 议与接收，意见的一致。
b) 由法律约束的意图。
c) 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 Borderless 衍生的 BDS 资产就不是金融工具。那么让我们看一下，我们能否能从 Borderless 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 BDS 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

Borderless 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，Borderless 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 Borderless 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 BDS 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。