BASTYON

基于区块链的真正去中心化的开源内容发现和社交平台

作者：Bastyon 开发者


BASTYON

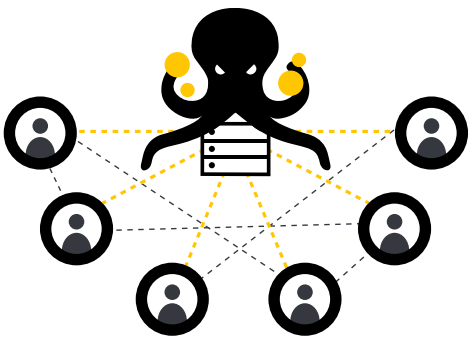
摘要:

互联网平台通过有效地将商品、服务和几乎任何类型的内容的创作者和消费者聚集在一起，解锁了令人难以置信的价值。然而，由于各种隐私问题和极端集权所带来的丑闻，这些平台正在失去用户。现在非常清楚的是，在当前的互联网环境中，几乎所有的权力和财富都集中在极少数人手中，他们缺乏传播财富的动力。这种权力被挥舞着用来保护领土、垄断、剥削有利可图的创作者（由于垄断，他们现在也没有什么选择）和任意审查。

Bastyon 将比特币的基础带到了互联网平台。所有由平台创造的巨大价值都在Bastyon生态系统的玩家之间，以透明的、可预测的方式共享。不存在任何一个中心化实体可以剥夺或减少创作者获得成功后的收入份额。每个创作者获得的 Pocketcoin 代币数量与他们对平台的贡献成功程度成正比。此外，用于自助广告的 Bastyon 直销市场允许买家们使用去信任的多签名交易，从特定创作者那里购买广告。广告可以是预先设计好的，也可以是自定义植入，创作者可以自由地展示广告。这与传统平台不同，因为在传统平台上，绝大部分财富都被平台的股东夺走了。

Bastyon 具有与这些成功平台（如谷歌、 Twitter、Facebook、Reddit、Snapchat、Patreon和维基百科）可媲美的元素，以及全新的功能。非法内容的监管是由平台参与者完成的，他们对平台的成功进行了可核查的投资。 发布、点对点通信、汇款、互联网搜索的整个过程都是基于运行 Bastyon 区块链的平等节点，并基于建立多种界面以适应不同用户的需求的可能性。大批用户正在迅速脱离传统公司发布和社交平台，他们将寻找可以拥有内容、订阅用户和获利渠道的平台。

The Old Way

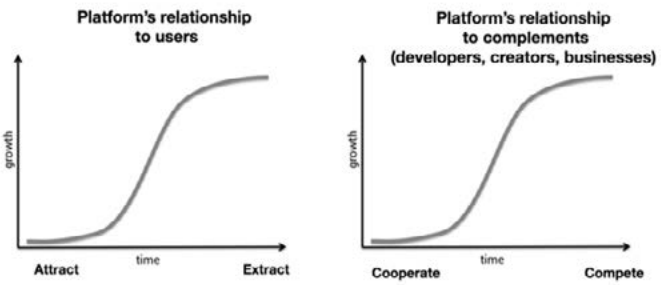


The Bastyon Way

作者：Bastyon开发者

1 互联网的现状

当前互联网平台的巨大盈利能力是基于平台设计中固有的效率，但回报和奖励被越来越多地控制并给到了平台的所有者，而参与者只能得到“残羹剩饭”，在平台的运营中没有发言权。创作者的收入增长速度远不如创造的价值（和平台的价值），算法被任意更改，以为平台创造新的收入来源，并且剥夺了用户的权利。平台收集越来越多的个人信息，导致经常性的违规和滥用。同时，平台的准垄断权力使他们以任意的方式控制言论，仅仅给出“使用条款”[1]中极小且难懂的条文而不做任何解释。一张图片胜过千言万语，没有比Chris Dixon提供的这张图片更能说明中心化平台的本质了。



来源：https://medium.com/s/story/why-decentralization-matters-5e3f79f7638e

[1] 需要明确的是，我们在这里并不是在争论平台不应该打击非法内容。口袋网（Bastyon）有一个内置的机制，由那些对平台的成功投入最多的人，即内容的创作者来监督内容。

口袋网(Bastyon)区块链

作者：Bastyon开发者

那么，我们怎样才能解决这个问题呢？答案：通过开放平台。口袋网（Bastyon）区块链和任何去中心化的加密货币一样，是由平等的节点运行的。但是，除了典型的加密货币代币转移外，还有其他一些交易：允许用户发布内容、为其质量点赞、推广和订阅创作者（包括加密的、只有订阅者才能看到的私人订阅）。登录口袋网（Bastyon）平台只需要被转换为12个关键字的私钥。用户可以使用该私钥与区块链进行交互。这种区块链方法有几个优点。如上所述，首先是经济去中心化，允许与节点持有者和创作者（价值的最终生产者）最大限度地分享价值。其次，也是令人惊讶的是，它的易用性。通过区块链，用户能够从任何设备上用他们的私钥登录，并立即从区块链中获取所有的个性化设置（无论是加密的还是公开的）。通常情况下，这个功能是去中心化平台的弱点，同时也是中心化平台的优势，也就是从任何设备/浏览器登录而不会失个性化设置。

口袋网（Bastyon）区块链是基于随机的权益证明（Proof-of-Stake）算法的。然而，有效节点需要执行几项服务。节点维护区块链，同时也响应来自前端的RPC套接字调用。

经济激励

由于口袋网（Bastyon）没有任何需要赚取利润的企业实体，所有创造的价值都由两组的生态系统参与者分享，也就是是内容创作者和节点操作者（也就是这个项目的开发者）。

- 内容创作者是由其公钥和选择性透露的关于他们自己的信息来识别的匿名用户。
- 节点负责支持生态系统中的各种服务（区块链、支持前端应用程序共享数据、防御女巫攻击）。这些服务超出了典型的加密货币节点的范围。节点被要求执行这些服务以获得奖励。

口袋网（Bastyon）区块链包含一个名为口袋币（Pocketcoin）的本地代币。就任何去中心化的加密货币系统一样，有两种方式可以使生态系统的参与者自然获得代币：一种是代币发行，另一种是交易费。

交易费：分享内容、点赞和订阅等许多交易都是免费的（但有数量限制，或者需要有余额以防止女巫攻击，见下文）。如推广内容之类的交易，则需要强制性收费。所有交易费用在节点操作者和内容创作者之间分配。

代币发行：口袋币（Pocketcoin）的发行量上限为24,375,000个。超过这个上限，将不会有任口袋币（Pocketcoin）产生。

Bastyon.com 接口

由于口袋网（Bastyon）是去中心化的，就如任何人都能建立比特币钱包一样，任何人都可以建立一个接口。但是，有一个由口袋网（Bastyon） 核心开发者团队撰写的口袋网（Bastyon）接口，作为进入口袋网（Bastyon）内容发现和交互区块链的第一条通道。有两种方法可以使用该接口：

1、使用Bastyon.com移动优化的Web App
2、使用口袋网（Bastyon）桌面应用程序。它是使用Electron框架构建的，与Bastyon.com Web App相同，只是

它通过代理服务器与各节点进行通信，而无需登录网站。

口袋网（Bastyon）界面是由屡获殊荣的开发人员和设计师构建的。目前支持以下功能：

1、在区块链上创建一个带有昵称/头像的个人档案
2、 在你的频道上发布内容
3、 以一至五星的标准对内容进行评分
4、 私人订阅和公开订阅
5、 要求以口袋币（Pocketcoin）和其他加密货币进行捐赠
6、 集成钱包，显示余额，以及基于其他人高度评价的内容所获得的口袋币（Pocketcoin）奖励
7、 对非法内容进行标记
8、 点对点、一对一聊天与群聊
9、 通过集成的PeerTube功能加载和观看视频
10、非同质化代币3.0 （NFT 3.0）

用户可以在任何设备上输入12个字的私钥助记符登录Bastyon.com。然后Bastyon. com拉取所有的个性化设置，如订阅、以前的内容分享和点赞，以及作为内容创作者所获得的口袋币（Pocketcoin）收入信息。因此，该系统是高度可移植的。

任何登录Bastyon.com的用户都会看到，基于订阅和系统中内容排名的整体算法所推荐的内容（见附录A）。

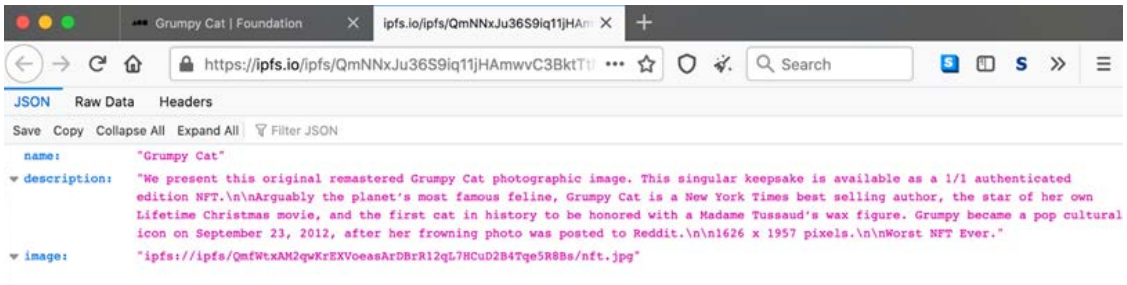
口袋网（Bastyon）的非同质化代币3.0

作者：Bastyon开发者

非同质化代币(NFT)在以太坊和其他区块链上迅速发展。推动NFT的价格和采用的主要想法来源于对数字 «房地产 «的所有权。然而，就其目前的形式而言，NFTs存在三个主要问题：

问题1：价值百万的404错误

NFT只是附加到区块链交易中一些元数据。在这个元数据中，是指向正在出售的实际艺术品的链接。这个链接是一个URL或网络上的一些其他标识。最近，相当多的NFT正在使用IPFS（星际文件系统）来存储文件。下面是NFT外观的示例（来源）：



事实上，NFT类似于口袋网（Bastyon）的社交交易，但有一个重要区别。口袋网（Bastyon）不仅有一个区块链节点，还包含一个配套的数据库（初始版本使用的是名为Reindexer的数据库，但到2021年6月，口袋网（Bastyon）计划切换到sqlite，以减少节点的RAM使用）。这个配套的数据库相当于IPFS，但只适用于口袋网（Bastyon）。事实上，口袋网（Bastyon）核心团队考虑过使用IPFS（正如许多其他项目所做的那样），但我们发现它有两个问题。问题1是链接会随着时间的推移而失效。问题2是维护IPFS文件的时间和金钱成本很高（显然，这源于问题1）。IPFS有自己的币，叫做Filecoin，所以除了以太币的GAS费之外，还有维护文件的额外费用。而且与以太币的GAS费不同，这个费用需要在几十年甚至更长时间内（NFT的整个生命周期）进行预测。

科技媒体The Verge上的一篇文章是这样解释问题1的：»不过，这个系统还是有缺陷的。Check My NFT背后的团队一直在研究和观察NFT，看看他们的IPFS地址是否真的有效，他们发现在一些情况下文件就是无法加载。该团队发现，主要艺术家的作品暂时丢失，包括Grimes、deadmau5和Steve Aoki。凯斯西储大学的法学教授、《所有权的终结》一书的合著者Aaron Perzanowski在给The Verge的一封电子邮件中写道：»这些文件最终在该团队提醒作品缺失之后又重新上线.....对于这些NFT的买家来说，这是一个非常昂贵的404错误。»（来源）

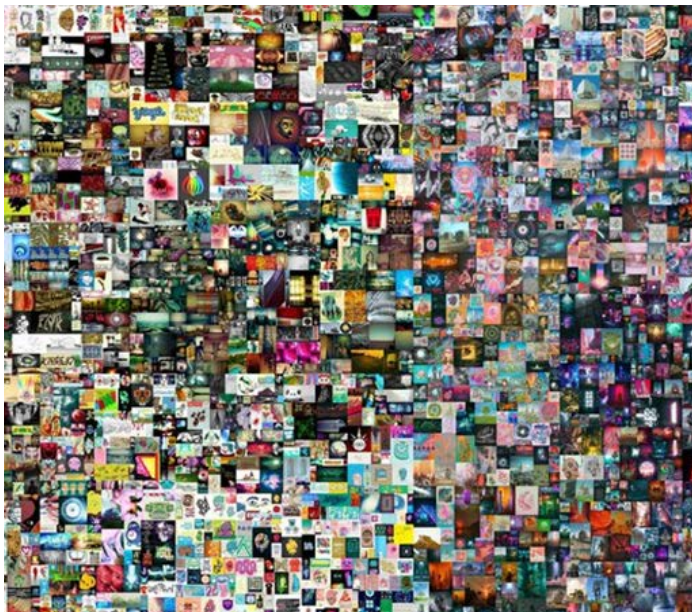
口袋网（Bastyon）通过构建解决了这两个问题。事实上，口袋网（Bastyon）上的每一个帖子都可以被看做一个原生的NFT，它真正具备NFT的所有方面，完全不依赖外部数据库。口袋网（Bastyon）交易有一个区块链组件和一个配套的数据库组件，后者存储在节点中的一个单独存储中，但它与区块链紧密相连，每一块内容都经过Hash散列算法写在交易中。而这就引出了问题2和及其解决方案。

问题2：NFT与区块链之间的松散联系

区块链中的交易通过元数据与实际的NFT有松散的联系。不存在连接的直接证明，许多URL的文件都可以更改。在口袋网（Bastyon）中，NFT的哈希值（Hash）存储在交易中，因此可以证明NFT是每笔交易中出售的实际NFT。

问题3：没有稀缺性

任何人都可以访问和下载NFT的内容。最近有人以6900万美元购买了Beeple NFT（见下图）。购买此图片只是拥有了特定区块链上的特定文件的权利。该作品不存在任何稀缺性，任何人都可以自由复制。



因此，NFT几乎没有什么独特性或稀缺性。但是因为在口袋网（Bastyon）中，NFT的两个部分都在同一个生态系统中，实际上是在同一个节点上，而且因为口袋网（Bastyon）已经包含了数字身份，我们还可以做另外一件将创造更多稀缺性的事情[2]。在口袋网（Bastyon）中，NFT的卖家可以选择只显示预览图（比如：图片的低分辨率版本），并拍卖加密的完整作品。然后，拍卖的赢家将获得所有权，并将获得解密作品的秘钥。但只有赢家能够解密，因为密钥将被加密到赢家的公钥。

以下是口袋网（Bastyon） NFT 3.0拍卖的步骤：

1、 在口袋网（Bastyon）上发布带有行动条款、元数据和实际NFT的帖子。口袋币（Pocketcoin）（PKOIN）的费用将由节点按照交易规模的比例进行评估。如果卖家选择加密完整的NFT，只显示预览，交易将包含预览，但完整的NFT将使用由（卖家私人密钥乘以交易ID）得出的AES密钥进行加密。
2、 竞价。对作品的竞价将使用哈希时间锁定合同(HTLC)。本质上，买家创建一笔交易，锁定与作品出价等同的PKOIN金额。该交易的有效期为拍卖结束后的一周，交易包含一个根据卖家的私钥、交易ID和重复散列所得出的哈希值。如果买家赢得拍卖，这个PKOIN将被卖家认领，卖家将在交易中出示散列的原像。如果需要增加出价，将只针对增加的金额进行额外的HTLC交易。
3、 卖家通过另一笔交易选择赢家。这也是

[2] 作者感谢能与 Sean Walsh 就这一话题展开富有成效的对话

一个哈希时间锁定合同（HTLC），但PKOIN的金额是名义上的。卖家包含与第2步中相同的哈希值。时间锁定是在拍卖日结束时加上3天。

4、 买家要求支付名义上的PKOIN金额，为此他必须透露上述第2步和第3步交易中的哈希值的原像。买家在拍卖结束后有3天的时间来要求中标并透露哈希值。如果买家退出，他将被阻止参与今后的NFT，并且以后节点不会接受来自该公钥的交易。

5、 卖家现在知道了第2步骤中交易的哈希值的原像，因此可以索要在第2笔交易中为NFT支付的PKOIN（加上包含相同哈希值的额外增加的竞价HTLC交易）。如果一个作品被加密了，那么这笔交易的元数据中也包括了加密到买家公钥的解密AES密钥，这样其他人就不能索取了。

总之，口袋网（Bastyon） NFT 3.0框架通过一个简单而直观的软件包中解决了当前NFT技术的主要问题。

口袋网（Bastyon）自助广告、直销市场、定制贴片广告

口袋网（Bastyon）将为内容创作者提供一个创新广告直销市场。每一位创作者都可以接来自广告买家的广告。为此，内容创作者可以选择加入市场，选择可接受的广告定价范围，向他们的订阅者展示广告内容（广告赞助内容会被标示）。广告买家可以在市场上看到内容创作者的报价，以及博客订阅者的数量、评价、最常用的标签和其他信息，以帮助广告买家决定该创作者和渠道是否合适。广告买家创建一个广告，并选择市场上的创作者名单（在考虑上述指标和成本后）。一笔交易被创建，由买家签署并发送给节点，其中包括广告信息，从广告买家到创作者地址的口袋币（Pocketcoin）输入。这样一来，交易对双方都是去信任且安全的，如果交易被验证并被添加到区块链上，就意味着双方同意交易，口袋币（Pocketcoin）被支付。这种自助的直销市场提供了极好的的目标定位机会，因为广告买家可以微调传递广告信息的实际创作者/博客。没有中间商，所以该服务非常高效，基本上是将广告买家和渠道方直接匹配。直销市场是一种机制，可以有效地提取平台创造的巨大价值，而不在中间商身上浪费时间。当作为激励机制的发行结束时，这种广告将给予口袋网（Bastyon）上的创作者物质激励，节点将通过口袋币（Pocketcoin）的多签名交易的广告费获得激励。

V 女巫攻击

作者：Bastyon开发者

去中心化平台的最大危险是女巫攻击。这个问题并不是口袋网（Bastyon）所独有的，甚至不是一般的去中心化平台所独有的，但比起依靠个人身份识别来对抗它的中心化网络来说则更加严重。简单地说，由于口袋网（Bastyon）账户只是一个可以任意创建的匿名公钥，我们需要确保这种僵尸账户不会影响到实实在在的内容创作者和消费者。口袋网（Bastyon）有两种机制来防御这种攻击。

账户余额。通常情况下，加密货币通过要求交易费用来降低女巫攻击的风险，从而使进行大规模不诚实行为的成本变得很高。然而，口袋网（Bastyon）是一个内容发现平台，要求即使是微不足道的交易费用也会阻碍任何形式的体验。因此，内容分享、点赞和订阅是免费的，但所有交易都需要口袋币（Pocketcoin）的余额。这限制了创建机器人军团的能力，因为这样做需要获得和持有口袋币（Pocketcoin）。起初，每个用户将能够在口袋网（Bastyon）上创建几个帖子和互动，而无需任何余额。在平台上发布高质量的内容将获得其他用户的点赞和代币奖励，这将使用户能够继续使用平台。从限制性会员身份转为正式会员所需的余额相对较少，只需发几篇高质量的帖子吸引评论就可以实现。

Antibot。我们在区块链上开发了一个独特的Antibot系统。由于我们的区块链是匿名的，所以很容易识别有余额的公钥的行动（加入口袋网Bastyon需要余额）。区块链分析系统被用来尝试取消用户的匿名化。我们是以一种完全不同的方式来使用它。在口袋网（Bastyon）中，Antibot平台将阻止超过特定活动限制的、类似于机器人活动的交易；这与现在所有集中式社交网络的做法基本相同。按照复杂程度递增的顺序排列，Antibot可以执行的限制包括：

1. 违反对特定公钥的发帖限制。每个限制性会员的公钥每天只能发15个帖子和45个评分。每个正式会员每天最多可以创建30个帖子和90个评分。
2. 禁止相互投票
3. 禁止对帖子进行点赞、反对、举报的组织行为

所有限制只是基于时间的。不存在对公共ID的封锁。从一个平台上消除所有的僵尸活动是不可能的；即使是依靠官方识别的集中式平台也很少能做到这一点。然而，我们的目标是使机器人活动得成本变高，高到他们意识到，在口袋网（Bastyon）上用合法的推广内容的方式其实更合理有效。

隐私

> 为了使隐私得到广泛传播，它必须成为社会契约的一部分。人们必须为了共同的利益而一起部署这些系统。隐私只扩展到社会上同伴的合作。
>
> 密码朋克宣言

隐私对于口袋网（Bastyon）和其他许多去中心化的网络都是至关重要的。然而，任何一种社交网络都需要进行制衡，以确保不诚实的行为者不会通过滥用规则而将系统变成一个污水池。我们认为这并不是无法解决的矛盾，而是创造性的张力。

口袋网（Bastyon）的隐私机制

1、匿名。与大多数区块链一样，公共身份是匿名的。然而，如果用户想保持身份（公钥）的信誉，用于发布内容和与口袋网（Bastyon）区块链交互的身份是固定的。同时，用户可以随时丢弃一个公钥，并启用一个新的具有空白信誉的公钥。
2、订阅。属于某个公钥的、对特定内容创作者的标准订阅，在区块链上是可见的。但是，可以使用私人订阅，区块链中的同一订阅通过256位AES密钥进行加密，该密钥通过加密散列从口袋网（Bastyon）私钥中派生出来。这样，当用户登录Bastyon.com时，客户端代码可以获取并解密订阅内容，以显示适当的内容，而不会向外界透露。
3、聊天。口袋网（Bastyon）的聊天是点对点加密的，使用的是口袋网（Bastyon）公钥派生的的密钥。因此，在群组聊天或私人聊天中的信息是私密的。
4、内容分享和公钥点赞在区块链中是可见的，并与化名绑定。
5、与Bastyon.com上的内容的任何互动（除了发布和点赞）都是私人的。换句话说，别人无法追踪你搜索和点击的内容等等。

因此，口袋网（Bastyon）不是匿名的。然而，它提供了强大的隐私保护和机制（如Antibot），使滥用此类隐私的行为成本变得昂贵。

非法内容和垃圾信息

我们已经了解到Antibot系统将使该网络的垃圾信息难以扩散，有可能达到和任何集中式社交网络一样的成效。

那么非法内容或色情内容怎么办？当用户第一次登录时，他们会看到以下规则。

口袋网（Bastyon）社区规则：

- 点赞优质内容，你的点赞很重要
- 为你的内容上添加适当的分类和标签
- 不得有任何形式的色情内容
- 不得有暴力威胁
- 对质量差的内容予以反对和降权

口袋网（Bastyon）采用了一种方法，该方法已经被维基百科和其他知识平台成功应用。每一位具有足够高信誉的用户都可以标记任何帖子。我们鼓励用户对违反规则的内容进行标记。该内容不能是个人不同意或个人觉得反感的内容。如果用户仅仅只是对某些内容感到反感，只需要屏蔽该用户。当然，被打上一个甚至许多标记并不会使内容从平台上消失，必须达到足够的高信誉用户之间的共识。以下是相关规则：

6、如果有50个标记，并且5星表决和标记的比率（都只来自高信誉用户）低于5，那么该账户的交易在1周内将不被接受到节点中。
7、如果这种情况在任何3个月内发生两次，该账户将被封锁3个月，其信誉将被清零。
8、同一组高信誉的用户不能在第一阶段（一周封杀）和第二阶段（三个月封杀和信誉损失）影响同一个账户。换句话

说，我们不允许一个群组协同攻击某些账户。

9、高信誉的用户将在他们的应用程序中看到特殊的标签，上面写有标记的内容和潜在的僵尸网络共谋者。所以，我们的设想是，高信誉的用户对平台的成功有足够的投入，可以以版主身份履行责任。头两年对该框架的测试表明这个设想是正确的，到现在口袋网（Bastyon）依然没有色情或威胁的内容存在。

发行量

口袋币（Pocketcoin）的总发行量被固定为24,375,000。一旦达到这个数字，将不再发行口袋币（Pocketcoin）。

口袋网（Bastyon）将不会有ICO。但我们将需要一种方法来吸引初始用户，然后再启动病毒式增长机制。口袋网（Bastyon）也需要激励初始开发人员，因为他们将只收到口袋币（Pocketcoin）。因此，我们在初始阶段设置了更多发行量，即：对于前75,000个区块中，发行量为每个区块50个口袋币（Pocketcoin）。这等于每个区块的初始比特币发行量，但区块的产生频率是原来的10倍。因此，在75,000个区块阶段，发行量为375万POC。在第75,000个区块后，长期发行量切换到比特币的长期发行量，即每区块5个POC，1分钟一个区块（所以每10分钟50个POC），然后在210万个区块后，每区块2.5个POC（同样，因为区块产生频率比比特币的高10倍，切换发生在210万个区块后，而不是像比特币的210,000块）。

95%的发行量用于节点、视频服务器和聊天服务器，5%用于内容创作者。

口袋网（Bastyon）扩展：视频和P2P聊天

口袋网（Bastyon）区块链不仅为社交网络活动创建了一个中央账本，还能够整合其他服务，如视频平台和P2P聊天。中心化的平台的一切都通过由企业实体控制的中央服务器完成。去中心化的基础设施，如torrent，历来繁琐、缓慢且不可靠。去中心化平台的问题的核心是公地悲剧以及无法维持一个标准。口袋网（Bastyon）是这样解决这些问题的：

1、当一个公共免费资源被玩家们自私地过度使用时，公地悲剧就会发生。举个例子，假设有一个公共视频服务器（如，PeerTube是一项去中心化的视频技术），运行这样的服务器是一笔不小的费用，而且这笔费用是由单个发烧友承担的。随着时间的推移，用户需要更多的存储空间。一些人可能会赠送给一些利他主义者，但随着时间的推移，会有更多“蹭”服务器的人。于是，服务器被关闭，视频消失，平台体验被破坏。在口袋网（Bastyon）中，口袋币（Pocketcoin）及定向发行到节点的能力，创造了一种为视频服务器的服务付费的方式（P2P聊天服务器也一样）。但现在我们有了第二个问题：如果收了费服务器却消失了怎么办？

2、当去中心化的服务器没有提供良好的正常运行时间或可靠性时，且无法靠人的力量解决时，就无法维持标准。每个视频或聊天服务器都会在区块链上注册，并抵押一些口袋币（Pocketcoin）。然后，可以通过提供服务获得口袋币（Pocketcoin），但前提是服务器在正常运行时间和质量上广受好评。评价信

誉是由用户的特别投票得出的。举个例子，如果有人观看了在区块链中与某个服务器公钥绑定的视频，速度慢得惊人（或者视频根本无法加载），该用户可以给服务器一个1星的评分，从而降低他们的报酬。如果评分过底，该服务器就会被禁止提供服务，他们就会损失抵押的口袋币（Pocketcoin）。

3、第三个问题是冗余。在许多去中心化的平台中，一个服务器存放内容或提供服务，不会有冗余。在口袋网（Bastyon）中，去中心化的服务器形成集群，一个集群中的所有服务器相互支持。每台服务器通过公钥和一种叫做rendezvous hashing的一致性算法被分配到一个集群。这确保了在新的服务器进入或离开平台时所产生的干扰最小化。

总结：口袋网（Bastyon）是一个去中心化的社交网络和通信系统，支持发布、评论内容、上传视频和p2p聊天的功能。口袋币（Pocketcoin）是一种网络代币，可以用来推广内容、购买广告、购买特殊的个性化功能（字体和皮肤）。口袋网（Bastyon）由高信誉用户以去中心化的模式来管理。在当前审查制度猖獗无度的环境下，口袋网（Bastyon）提供了一个稳定和可扩展的方式来维持社区交流，同时将不受欢迎的内容拒之门外。

附录A：基于价值的信息流

任何人都可以不经身份验证加入口袋网（Bastyon），所以如果帖子按时间顺序排列，则很容易被滥用。这就是为什么开发人员执行了一个基于价值的信息流程序。以下为计算方法：

口袋网（Bastyon）最初是纯粹按时间顺序排序的。在设置中可以选择按时间顺序展示，但默认排序是基于质量的。我们将帖子的质量定义为：

讨论：简单来看，我们可以把公式的左边（0.6以下的所有内容）看成与用户信誉有关，右边则与实际的帖子本身有关。这个公式的总体目标如下：

.4*[(.75*(LAST5R+BOOST)+ .25*REP)]*DREP+.6*POSTR*DPOST=POSTRF

LAST5R — 在24小时内帖子的5星评价数量的百分数

BOOST — 指在一定数量的区块内所有活跃速推（Boost）的百分数（目前这个数字是500）。有一个上限，超过这个上限，加钱速推就没有用了，口袋网（Bastyon）界面会显示这个范围（与谷歌AdWords等传统广告中的出价范围类似）。在这个框架下，更高的出价将在信息流中获得更高的广告位置。

REP — 该用户在所有用户中的声誉百分数

DREP — 与信誉相关的参数和速推（Boost）的衰减率（等于0.7）

POSTR — 过去24小时内的帖子评分的百分数

DPOST — 帖子评分的衰减率（等于0.96）

*所有的评分仅来自信誉高于目标水平的用户

1、 高评分的帖子应该在信息流顶部区域停留更长时间，为用户提供更高质量的体验。这是通过给予公式右侧超过1/2的权重和提高DPOST衰减率来实现的。公式左侧的与信誉（比率0.7）相关的衰减公式将在大约12个区块内归零，但帖子的衰减（比率0.96）将在超过100分钟后才归零。
2、 公式左侧关于信誉的部分不应过度给用户信誉过高权重。在口袋网（Bastyon）不应出现如下情况：内容质量下降了，但过往的信誉评价仍使之排在信息流的顶部。所以，在公式左边，用户信誉的权重仅为0.25，而用户最近5次评分的信誉权重为0.75。由此可见，重要的信誉评分来自于用户最近创建的内容。
3、 Boost本质上相当于给LAST5R（用户最近5个帖子的5星评价数量）进行了助力增长。

附录A：规模化

建立任何内容发现和社交平台的一个主要因素是规模化。区块链真的可以处理一个拥有数千万或数亿用户的平台所需要的量级吗？我们认为，相对简单的增强功能可以轻松地服务于数千万用户，而更基本的增强功能可以将这样的系统扩展到几乎任何水平。扩展去中心化加密系统的最大问题是（按照复杂度递增的顺序可以说是）：

1. 验证速度
2. 验证节点上的区块链存储
3. 网络和交易处理

我们以比特币为例，因为口袋网（Bastyon）的代码是松散地基于比特币核心的。每10分钟有1兆字节的区块，假设交易大小为250字节，则每小时有24000笔交易，24小时有600000笔交易。这对于像口袋网（Bastyon）这样的系统来说是远远不够的。如果我们假设每个口袋网（Bastyon）用户每24小时会进行5次链上操作，那么600000的限额就只有11.6万名用户。然而，并不是所有的东西都会丢失。如果我们仔细看一下不可转让代币（NTTs）的类型，会发现它们非常适合我们所说的自由基聚合。为此，我们将需要两个已经在加密货币世界中确立的概念：Schnorr签名和隔离见证[3]，再加上对区块中继和接受进入等待确认的交易集合的可能改进。例如，我们想一下在口袋网（Bastyon）上对用户发表的帖子进行评分的行为。从长远来看，我们只关心帖子的评分方式，我们并不在乎是谁评价的。因此，我们可以将所有的评分汇总成一笔交易，如下图所示。区块的黄色部分包含了所有由用户进行的«评分«交易。每个单独的评分交易可以有100个字节。这类交易的数量可能非常多，当平台规模达到Twitter、Reddit的水平时，每秒可能有数千笔交易。如果平台有5千万用户，他们每

[3] 隔离见证是首次在比特币中实现的一项功能，它将区块链分割开来。隔离见证中，有一些涉及了交易的基本含义的必要数据，以及可以丢弃的数据。比特币中的永久数据是描述谁给谁付款，瞬时数据是交易验证所需的签名，但一旦它在区块链中足够深入，区块链的整个性质表明它们已经被验证了。

人每天平均给5个帖子评分，这意味着平均每秒有2894笔交易，每天有2.5亿笔交易。

Main Block

One Transaction including
(for each post rated in the block)
1. Offset reference to original post on the blockchain (~32 bits)
2. Number of ratings for the post in #1 (~32 bits)Total ~8 bytes

Extended Block

Transaction for each post (#TXs = num posts*num ratings)
1. Pubkey of rater (33 bytes)
2. Offset reference to original on the blockchain (~32 bits) *Num Block + Num TX
3. Schnorr signature for pubkey in #1 (64 bytes)Total ~ 100 bytes

现在我们来分析一下口袋网（Bastyon）在规模化的三个关键维度上的情况：

1、验证 – Schnorr 签名有一些令人难以置信的批量验证特性。在合理的个人电脑上，Schnorr签名可以以每秒近20,000笔交易的速度进行验证。根据比特币核心开发团队的研究，批量验证可以将速度提高2倍，达到每秒1,000次验证的速度。因此，Schnorr签名可以允许每秒40,000笔交易，所以这不会成为口袋网（Bastyon）规模化需求的瓶颈。

2、在验证节点上的区块链存储 – 要知道在主区块中，我们只保留被评分的帖子的参考信息和评分总数。所有的支持信息都在扩展区块中。扩展区块要比主区块大得多，因为它将包含每个帖子的每个评分的单独交易，但一旦这些评分被验证并保存一到两个月，扩展区块就不再被需要了。我们之所以需要将每笔交易保存一到两个月，是因为口袋网（Bastyon） Antibot系统需要观察评分或发帖等行为。因此，最终，在区块的2分钟时间内被至少点赞过一次的每一个帖子将占据8字节的存储空间。注意，我们参考的是原始的帖子交易，而不是在每次评分时将它的URL或哈希添加到区块链中。截至2018年，Facebook用户每分钟产生400万个点赞。即使是如此巨大的活动量也可以被容纳在仅仅16MB的数据中。但我们的目标不是Facebook的量级，因为口袋网（Bastyon）上的讨论是在一个去中心化的点对点聊天中进行的，从来没有存储在区块链上。在这个意义上，它类似于Snapchat，因为信息会在一段时间后完全消失。总而言之，口袋网（Bastyon）与Facebook不同，我们甚至不想以达到这种几乎无意义的点赞量级为目标。口袋网（Bastyon）上的活动可能更接近Reddit，Reddit上每天有5800万次的内容投票。平均来说，这意味着每个区块包含80,555个评分交易，这只需要大约160KB的存储空间，这是一个非常可控的量级。当然，系统上还有其他交易。例如，帖子本身需要有共

享的URL的160位哈希值，和帖子内的评论以及32字节的发帖人的公钥。Reddit每月有1100万个帖子发布，所以每天只有大约37000个帖子，每两分钟是51个。由于一个区块中的所有帖子将以类似于评分交易的方式进行汇总，每个区块的总存储量将是102*52字节，即5.3千字节。事实上，公钥也确实需要存储，可以用一个偏移指标来代替，也就是密钥第一次出现在区块链中的位置（第一次在区块链上发布内容除外）。

当然，实际的帖子并不在区块链上（只有其哈希值会出现）。它进入一个外部数据存储（也存储在一个极快的内存数据库中，以便访问[4]），与区块链同步，并对其进行验证。该数据库表中的所有帖子将保留3个月，之后只保留最受欢迎的帖子，以保持口袋网（Bastyon）搜索引擎结果的高质量。最终，当口袋网（Bastyon）达到像Reddit这样极高的全球流量时，帖子的数据库表实际上可以分布在各个节点上，但用户的数量需要达到数亿才有必要这样做。区块链仍将存储在每个节点上，所以除非发生哈希冲突，否则不可能为口袋网（Bastyon）上的帖子创建欺诈性评分。

3、区块传播-这一直是一个关键的绊脚石，然而它已经随着比特币核心的紧凑区块和比特币无限（BU）的Xthin区块等改进而得到解决。比特币矿工还成功地利用了快速中继网络，该网络使用户数据报协议（UDP）作为互联网传输手段，而不是较慢的TCIP协议。请注意，在实践中，大多数节点已经看到了全部或绝大部分的交易，所以这些交易不需要通过网络发送两次。这大大降低了节点之间通信所需的总带宽。

总而言之，口袋网（Bastyon）的具体设计允许它展开激进的规模化，与拥有数亿用户的大型社交网络同场竞技。

[4] 口袋网（Bastyon）核心开发者是受到了Reindexer的启发，Reindexer是Oleg Gerasimov建立的一个速度惊人的开源内存数据库 *https://github.com/Restream/reindexer*