ContentBox

一个区块链赋能的数字内容生态系统

CASTBOX.FM

2018-03-31

Contents

目录

项目背景

数字时代下的挑战

近十年来，在数字内容产业，我们见证了一次由 Reddit，YouTube 和 Spotify 这类网站和移动内容平台引领的爆炸式增长。这些音频和视频流占据了全网 70%以上流量，已成为我们日常生活中不可或缺的一部分。但是，数字内容产业的繁荣发展是建立在中心化平台的基础上的，随着数字平台话语权和流量的增加，基于平台生存的内容创作者、消费者和广告商却面临着来自中心化模式的威胁和挑战。

•内容制作者获利难。在传统的中心化数字内容平台上，想要对优质的内容进行打赏是一件非常困难的事。创作者在诸如 YouTube 和 Instagram 等内容平台上进行创作，而平台则利用这些作品贩卖广告从而获利无数。 这样一来，即便内容是平台最有价值的资源，其创作者获得的收益却微乎其微。虽然，头部的创作者拿到了属于他们的报酬，繁冗的平台费用却已经占据了大部分的收益。个人创作者或中小型机构因受制于支付条件和流量限制等因素，则始终处于弱势地位，议价能力严重不足。大部分情况下，则是由平台分掉利润大头，而创作者，尤其是中小创作者仅仅拿到了剩下利润的很少一部分。 例如：当一首歌曲被听众购买，只有 15%的利润被分给原创作者，85%以上的利润则进入了网络服务平台和发行公司的腰包。

•内容消费者无法获得收益。对于内容平台而言，让用户参与各种各样价值导向的活动是至关重要的，但后者从未获得经济回报。用户用他们宝贵的时间来和平台互动 (点赞, 投票, 收藏和评论等), 正是因为他们的参与，好的内容才得以被甄选出来，可他们却不能因此而获得应有的奖励。用户在无意中付出了免费的服务，却被诸如 YouTube 这样强大的内容平台利用而获利。在平台内部或外部的分享为平台带来了更多曝光度和流量（例如：在 YouTube 或者 Facebook 上分享视频给粉丝）.网络上充斥着各种质量或类型参差不齐的视频. 因此，如今稀缺的不是内容本身，而是用户的注意力。一个用户愿意花多少有限的精力在内容上——包括广告，是弥足珍贵的。

•内容平台之间的激烈竞争。 因为关键的用户信息和内容被平台锁在了他们自己的数据库里，所以让内容平台相互信任是几乎不可能的，这就导致了数字内容产业的残酷竞争。大型内容平台一掷千金来买下流行内容的版权也并不称奇。在抬高了竞标者成本的同时，也让中小型平台别无他选而只好放上低质亦或是盗版内容。这些居高不下的成本将会转嫁到最终用户上，导致更长的广告时间或是更高的订阅费用——最终降低了用户的体验。

基于区块链的社区生态系统

针对以上问题，我们推出了 ContentBox 平台，旨在为未来的数字内容产业构建一个以区块链为基础的社区生态系统。基于 ContentBox，数字产业将会迎来三个革命性的变化：***共享内容池，共享用户池，一个统一的支付系统。***

与传统的开放社区如 App store 或者微信开放社区 [1]不同的是, ContentBox 是一个完全**去中心化的，自主的，由开源社区**所驱动的平台。ContentBox 将会帮助用户以更积极的方式在各式各样的 Web 端和移动端分享数字内容以及带来一个无需第三方参与的快速转账系统。

原则上讲，ContentBox 致力于让所有内容产业利益相关者获益，包括但不仅限于内容创作者、消费者、广告商、分发商和应用开发者等。在这个生态系统里，这些利益相关者可以在公平开放的数字内容平台上进行创作、参与、合作和创新。

对于内容创作者而言，每当他们的作品被用户消费时，就会获得由支付系统提供的相应奖励，从而激励他们创作更多优质的作品，而那些作品极为受欢迎的创作者将会获得巨额回报。此外，ContentBox 实现了平台交易程序的极简化和自动化，内容创作者和粉丝可以脱离中间商直接交易。

对于消费者而言，他们会基于个人对社区的贡献而获得奖赏，包括分享、评论、投票……甚至是举报垃圾信息，只要这些行为有益于社区他们可以用所得 token 消费内容，譬如观看一部电影或下载一首歌曲。事实证明，当社区的发展前景与用户有直接关系时，他们便会投入更多的金钱和精力对其进行管理和宣传，比特币社区的崛起就是一个很好的证明。
广告商当然也可以在这个新的生态系统里获益。传统的广告商基于发行商发布的数据报告计算收益，但ContentBox提供一个可共享的广告统计账本，系统会按照实际的广告浏览量，以智能合约的方式自动支付广告费用。因为分布式账本是完全开放的，所以广告商可以随时自主查账。这种模式可以帮助他们构建一个整体和统一的营销策略，而不是在不同平台同时做很多推广活动。除此之外，他们还可以用token发起赏金计划来降低成本。

[1] https://open.weixin.qq.com/

对于分销平台和社交网络而言，他们可以共同构建一个共享的内容和用户分布式账本，而这将会通过降低支付给搜索引擎的费用和 IP 购买成本，来让每个人收益。他们可以把注意力放在增强用户体验，而非与其他平台的竞争上。

对于 APP 开发者而言，他们可以利用 ContentBox 的区块链 token、去中心化的支付基础、以及身份识别服务来构建用户体验更佳、变现能力更强的应用程序。

综上所述， 通过改变如今在数字内容产业里的规则，整个产业，包括所有的利益攸关者，会因为通力合作和公开透明而蓬勃发展。这将会迎来一个全新内容经济时代。为了培养和所有利益相关者的合作关系, ContentBox 将会发行名为 **BOX** 的 token，而这将会是社区经济的关键角色。

关于Castbox

Castbox 是全球最受欢迎的音频平台之一， 在谷歌商店里的新闻&杂志类紧随 TopBuzz 和 Twitter 排名第三。基于业界领先的音频搜索系统，Castbox 为播客和听众推荐所需的音频和有声书籍。如今团队发展超过 50 人，在北京，旧金山，纽约和香港均设有办公室。

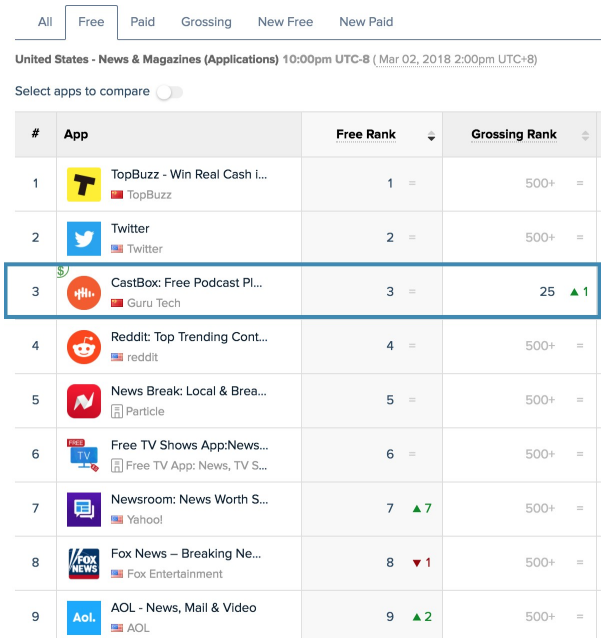

图 1: 新闻和杂志类排名，谷歌商店, 美国 (数据来源: App Annie)

Castbox 在 2016 年初由谷歌前员工创立，收录了全球 130 多个国家和地区 5000 万个音频节目，获评 2017 年谷歌商店最佳应用 。2016 年 10 月，Castbox 被评为了 Google Play 上的全球最佳热门应用，并获得了一系列其他奖项。Castbox 被 135 个国家列为谷歌商店编辑推荐应用。

基金会

ContentBox 基金 (下简称基金会)是一个非营利组织。它的成立是为了确保运行在 ContentBox 平台上的全新生态系统保持良性增长和创造力。 基金会将会管理收益的合理使用，并确保 BOX token 的正常流通。其终极目标是为数字内容产业打造一个完全去中心化和自动化的生态系统，基金会的管理和运作会尽可能地实现透明化。**长远来看，基金会将最终演变成为一个完全由软件所管理的组织。**

作为基金会的创办成员， Castbox 将会探索性地，从一个中性化的 APP 演变为一个基于区块链去中心化的 APP。并向数千万用户介绍 BOX token 来帮助提升用户体验，并且让他们享受每一次消费，创造，分享数字内容时所带来的乐趣。在不远的将来，BOX 系统被成功地整合进 APP 之后，Castbox 就会开放目前的大部分代码库，以鼓励开源社区驱动 ContentBox 平台的迭代进化。

技术架构

为什么需要一个新的区块链系统？

数字内容产业的性质决定了需要打造一个量身定制的区块链系统。

- **高频率.**数字内容产业在支付和行为频率上和传统的电子商务大有不同。 通常情况下，一个普通人在一天之内不会有多次转账或者买卖货物的行为。但在数字内容平台里，一名用户在几分钟内下载一首歌，观看一个电影剪辑或是打赏作者一篇文章等是很常见的。毫无疑问，我们期望服务着数百万用户的数字内容世界有更大的交易量。 而这需要底层的区块链系统具备能够在每秒钟之内处理数百次甚至数千次的转账吞吐能力。
- **隐私保护的高要求.**像以太坊这样的公链之所以有吸引力在某种程度上是因为它们的透明度: 所有的智能合约被公开的储存在每个节点上并且是独立可审计的。但是，在数字内容平台上的用户更倾向于进行匿名转账。 一个播客可不想见到自己的收入信息流向与交易无关的地方。 出于竞争和监管方面的原因，隐私对企业用户的交易来说更为重要。除此之外，正如DAO[3]事件和Parity[4]事件所揭示出来的那样——日益复杂的智能合同的可见性

带来了严重的安全风险。

- **普遍的微支付.**可以预见的是大多数的内容转账情况都是以小面额的形式进行的。例如，用户予以内容创作者小额打赏，或者是购买诸如流行电视节目的一集这样的付费内容。行业需要一个无缝微支付的解决方案来构建一个健康和生机盎然的社区。而这就意味着区块链的交易费用要被降到最低，甚至是零费率。

显然，像比特币和以太坊这样的主流区块链目前来看并不能够和数字内容产业完美契合。因此，寻求一个全新的解决办法来构建一个轻量级可扩展的区块链是解决上述痛点的必由之路。诚然，许多新兴的项目声称他们可以解决上面的问题，但是没有一个能够被证实会有成熟的产品上线，或者有足够的用户和开发人员来形成一个可扩展的、自我发展的生态系统。为了解决上述挑战，我们提出一个由三个主要组成部分所组成的体系结构：

- **BOX Payout** . 一个安全快速用来承载跨应用的多方安全支付服务的区块链系统
- **BOX Passport** . 一种基于区块链的跨应用跨平台的统一的身份认证系统。
- **BOX Unpack .** 一个帮助中小型企业轻松快速建立起一站式内容管理的解决方案。

接下来我们将用几个章节详细说明上述的三个组成部分。

预期目标和原则

在开始深入讨论核心部分之前，我们想要简单的介绍一下在 ContentBox 平台的设计中所考虑到的目标和原则。

简单来说，ContentBox 架构的主要设计目标如下：

- 当内容量和用户数量迅速增长时，能扩展
- 为内容产业设计出最常用的智能合约
- 保护转账隐私
- 支持微支付
- 轻松地与现有应用进行整合

[2]https://www.coindesk.com/dao-attacked-code-issue-leads-60-million-ether-theh/
[3]https://cointelegraph.com/news/lessons-from-parity-attack

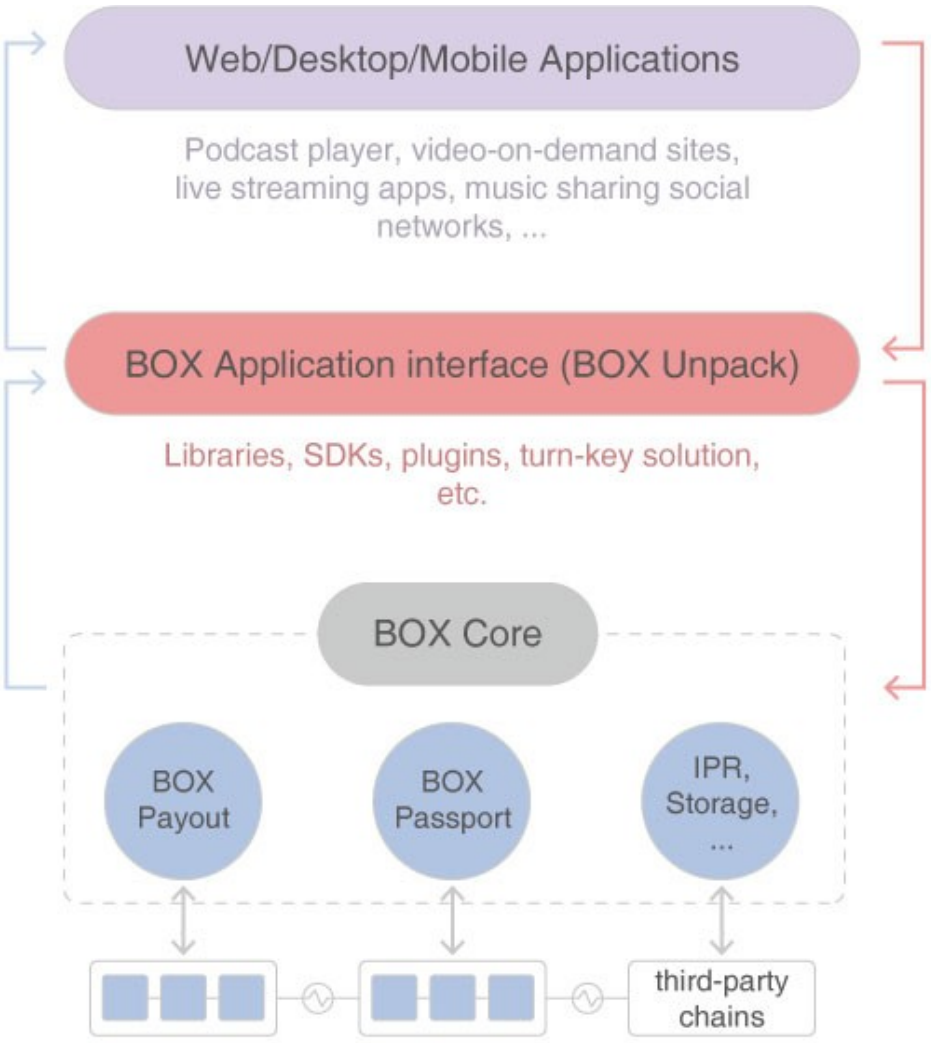

图 2: ContentBOX 架构总览

从概念上讲，上述所有的目标都可以通过设计一个更强大，功能更完善的，兼容 EVM（以太坊虚拟机）的区块链来实现。但是，ContentBox 并不希望通过构建一个庞大冗余的区块链系统从而实现预期目标。ContentBox 遵循 **UNIX 哲学**，即： 在一系列简单的，模块化的，可靠的小部件上建立一个大的系统，从而使整体更容易被调试和迭代。

除此之外，ContentBox 尝试通过其设计来让整个系统对开发者友好。一个生态系统不能仅通过其技术优势来笼络人心，更重要的需要赢得用户和开发者的信心和信任。因此，在 ContentBox 中的另一个适用原则是避免闭门造车，从头再来。而是直接利用已经过验证的、广泛使用的、最成熟的技术堆栈。

另一个重要的原则是保持**正交独立**的概念。我们的目标并非构建一个难以实现和难以应用的多重目标的区块链。此外，我们不希望两个组件套用同样的功能，这可能会使应用程序开发人员感到困惑。**正交独立性**使我们更容易理解事务结合时所发生的事情。

BOX Payout

一个毋需虚拟机的公链

BOX Payout 并非一个符合广义图灵完备虚拟机的区块链。主要原因是 BOX Payout 区块链支持在快速和安全条件下的交易，而这在数字内容产业世界里是很重要的。毋庸置疑的是，一个和以太坊虚拟机（EVM）相似的图灵完备虚拟机可以承载任意条件下的交易并确保转账的执行和完成，但它可能并不总是最优解。

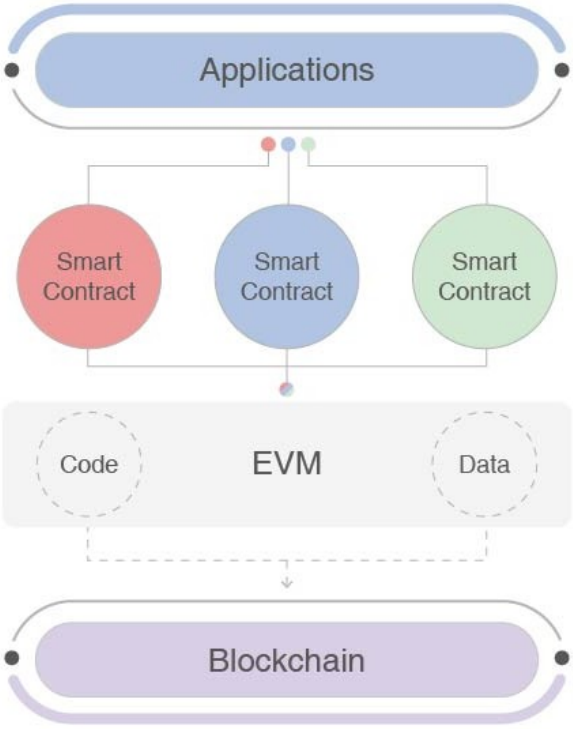

图3： 传统的链上智能合约。应用通过EVM和区块链的互动

在数字内容领域内，之前所展示的一个简单的有条件的交易通常涉及到一名用户，一个内容块和一个平台。为了执行这一多方支付，可以拟定一份智能合约来管理对各个部分的 token 转移，让 EVM 执行命令并验证结果。

显而易见的是，这是一个非常耗费资源的方法。随着内容日趋多样，对智能合约多样性的要求也随之而来，从而给区块链带来了沉重的负担。这是因为每个合约在每个节点上都会被执行。但幸运的是，由 Andrew Poelstra 这一 BlockStream 科学家所发起的研究和并在密码学领域内所取得的进展揭示了毋需虚拟机就可以达到相同效果的另一种解决方案——我们称之为加密合约。

加密合约

从本质上来说，加密合约是一种可以被翻译成一系列加密原语的智能合约。开发者也可以简单的认为它就是链下的智能合约。

自以太坊诞生以来，智能合约已成为众多区块链项目里不可或缺的一部分。但是，大多数合约所需要仅是区块链的一项功能：即基于交易不可更改的信任基石来防止双花。因此，与其使用复杂且资源密集型的智能合约来协调利益相关者的收益和执行相关自动化支付的事务，我们可以将简单的签名聚合起来以实现相同的目标，但是性能要高得多。

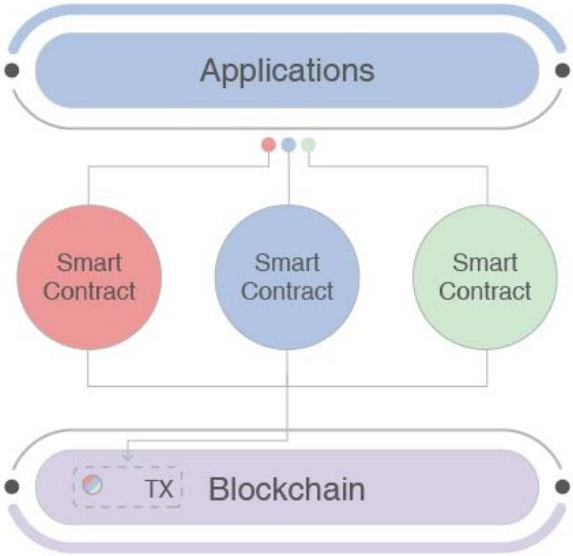

图4: 链下智能合约. 应用直接与区块链进行交互

基本上，一组参与者可以决定他们想要执行的某种合约或协议。因此严格地依照执行结果，他们将产生一个有效的签名，区块链及其校对机可以验证此签名是否有效。区块链并不需要知道原始交易的任何细节。通过使用签名本身作为证明，大量的交易可以被移至链下并让**区块链执行它真正擅长的事情：核查多重签名。**换句话说，一条智能合约可以被编译成一系列加密原语。当某人用这些原语签署并激活一次普通的交易时，虽然该智能合约并未托管在区块链上，但其仍然会被严格执行。

此方法的一个关键部分就是 Schnorr 签名。与 ECDSA 签名不同的是，Schnorr 签名在其自身的数学语言中具有线性性，这使得它非常适合创建“适配器签名”，可用于自动处理链下事务。通过用聚合的单个签名来替换嵌入在每个输入端的签名，区块链可以节省大量的磁盘空间的同时，也变的更轻量级，也比以前更强大。

举一个简单的例子：Alice 想要点播 Bob 所拥有的在线电影，然后她想支付给 Bob 1BOX 买下电影的一次性访问密钥。现在假设 Bob 在一个秘文 t 中嵌入了使用权密钥，而 Alice 得到 t 的过程可以描述如下：

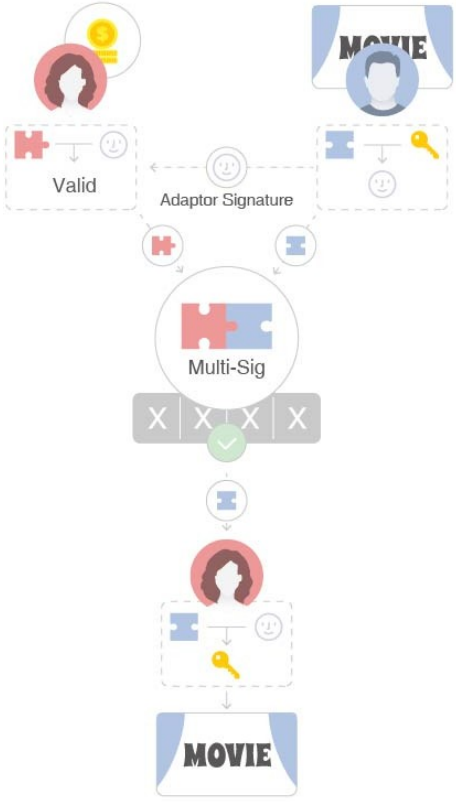

图5: Alice向Bob付款以获得一个带有适配器签名的影片访问密钥

1. Alice和Bob构建共同密钥 $J(A,B) = P_A^j + P_B^j$, where $P_A^j = H(H(P_A \| P_B) \| P_A) * P_A$,

   $P_B^j = H(H(P_A \| P_B) \| P_B) * P_B$ (P_A, P_B 为公钥)
2. Alice和Bob 共享 P_A, P_B, R_A, R_B (随机散点); Bob 计算 $T = t * tt$, 后发送T给Alice

[4] 技术路径图 - Schnorr 签名和聚合签名
https://bitcoincore.org/en/2017/03/23/schnorr-signature-aggregation/

3. 因此Alice和Bob同意随机的挑战 $e = H(J(A,B)||R_A + R_B + T||m)$ (H 表示散列算法, 这两个步骤没有显示在图上)
4. Bob提交适配器签名 $s^j = r_B + e * x_B^j$ (在图的右上角显示, x_B^j 是 P_B^j 的密钥)
5. Alice 验证: $s^j * tt = R_B + e * P_B^j$
6. 如果同意, 则Alice 给Bob发送她的签名: $s_A = r_A + e * x_A^j$ (x_A^j 是 P_A^j的私钥)
7. Bob完成后, 自动释放t: 首先，构建 $s_B = r_B + t + e * x_B^j$, 然后结合: $s_a = s_A + s_B$, 签署交易并在区块链上进行广播，然后 Alice看到 s_a
8. Alice做减法: $s_a - s_A - s^j = (r_B + t + e * x_B^j) - (r_B + e * x_B^j) = t$

共识机制

为了进一步提高 **BOX payout** 主网的可扩展性并使之提高移动端的友好度，主要的共识机制将采用一种名为网络效应证明(PoNE)的股权证明(PoS)衍生物。

PoS 是一种针对公链的共识机制，按矿工所持币数占整体代币数量的比例确定份额。在基于工作量证明中（ PoW ）的区块链系统里，由算法奖励解决密码谜题的参与者，以验证交易并创建新的区块。在基于 PoS 的公链里，一组矿工轮流对下一个区块提出建议并进行投票，每位矿工的投票权重取决于其股份的大小。

鉴于 ContentBox 平台服务对象的特殊性，PoNE 已被添加至普通 PoS 之上。被选择成为矿工的可能性大小取决于矿工存款的数量，内容创作和特殊节点的消费。与 PoS 一起，被选择成为矿工的节点得分计算公式如下：

$$_i\mu = \frac{s_i}{\Sigma_s} + \frac{c_i * \omega_i}{\Sigma_{(c*\omega)}}$$

μ_i 表示一个节点的分数

s_i 表示一个节点的股份

c_i表示一个节点的贡献分数，受与此节点相关的内容贡献的数量和频率的影响

ω_i 是一个非常类似于学术界所使用的影响因子权重值

为了在 **BOX 支付**区块链上进行挖矿，节点需要绑定协议，并进行安全存储。每轮区块的产生，将会随机按顺序选中 5 个矿工，并按照上述公式列出分数。如果第一个选中的矿工离线并无法履行验证职能，第二个矿工就会替换它，并取代其位置。

这种共识机制的显著优势包括安全，降低了中心化的风险以及有效利用能源。交易吞吐量将会被极大的提升。在消费内容产品时能大幅提高用户体验度。例如，当播放一段音频时，时间应该被记录下来，由此产生的相关的支付，无论是来自广告还是订阅，都应该立即被分发回它们的合法持有者手里。这就是构建 BOX payout 的全部前提。

因为 ContentBox 平台的目标是数字内容消费市场，而现如今这通常发生在移动端，因此用最小的资源消耗对付大量的分布式矿工数量是非常有必要的。考虑到上文所述的消费模式，未来的节点将会在移动设备上出现。它们的特点是：计算能力可能不那么强，而节点的数量可能会达到数亿。这为使用 PoS 建立了基础，而不需要考虑到 token 的初始分配。

BOX Passport

随着 ContentBox 社区生态的日益壮大，将会有大量的应用构建在公链上。单个用户在所有的这些应用程序中都应该有一个唯一的标识，而不再需要在每个应用程序上再创建一个独立的身份。因此，ContentBox 将引入名为 ***BOX Passport*** 这一强大的***去中心化身份交互服务***。它允许用户仅使用一个单一的数字身份即实现可跨应用或网页从而进行无缝交易，并极大的提高用户的隐私保障，安全性和对自身身份信息的把控。

Box Passport 通过扩展钱包的概念来建立这种身份，并将个人信息(如声誉)与 Token 账户相互关联。这种服务本质上去中心化的，并非通过某个应用的中心化数据库来实现，从而降低了被攻击的风险。用户可以完全掌控他们的身份信息并决定谁有权限使用何种信息以及使用的期限。除此之外，***BOX Passport*** 可以把一个创作者与他的作品透明地、永久地绑定在一起，这将帮助他在数字内容世界中建立起持续的声誉。

基于 ***BOX Passport*** ，我们为生态系统引入了一种叫做 ***BOX Login*** 的全新的特质，而这会开源给社区里的每一位开发者。概念上和 FACEBOOK 登录类似，***BOX Login*** 支持用户以更安全便捷的方式登录 ContentBox 生态系统里的任一网页，桌面端应用或移动应用。但是，和目前的第三方验证系统不同的是，***BOX Login*** 是部署在区块链上的服务，不受任一组织或公司所控制。

第三方标识服务(如Keybase[5] 和uPort[6])可能会集成到验证服务中，以实现更广泛的交互操作性。

[5]https://keybase.io/
[6]https://www.uport.me/
[7]https://arxiv.org/abs/1606.07792

BOX Unpack

应用接口

BOX Unpack 是 ContentBox 的应用程序接口，包括一系列的开发库，软件开发工具包，命令行和基于 web 的工具来帮助未来的合作伙伴和开发人员来共同构建下一代数字内容平台。和以太坊不同的是，**BOX Unpack** 并不需要开发者学习新的程式语言来写智能合约，相反，我们允许开发人员轻松直观地使用熟悉的语言例如：JAVA, Go, Python 等等来集成区块链相关服务。

BOX Unpack 的主要功能包括以下几个方面：利用 **BOX Passport** 注册和登录，在 **BOX Payout** 创建和提交交易请求，上传和注册数字内容，帐户迁移和整合以及使用一系列的工具来进行区块链上的内容管理。需要特别指出的是，**BOX Unpack** 为可重复使用的模块封装了基于 Castbox 内部开发的 AI 算法。这能够帮助开发者在去中心化应用里运行一些高级的功能：

•音频内搜索.这是 Castbox 最近推出的一种新创的技术，它允许用户用更有效率的方式快速搜寻到他/她想听到的内容。传统的音频搜索是通过标签抓取和标题描述来实现的。但这总会被一些精明的主播所利用（我们可以在 App Store 搜索引擎优化中看到类似的事情）。但 Castbox 发明了一种新的方式来执行搜索：它使用自然语言处理（NLP）算法来转录语音音频内容，并结合机器学习，依照每个用户的搜索和收听习惯来定制个性化的推荐结果。通过使用这项技术，ContentBox 上的开发者就能够开发出一个快速且智能的搜索引擎，可帮助用户在多个数字内容平台上发现有趣的内容。

•基于深度学习的推荐引擎. Castbox 的推荐引擎是基于目前 Google Play 所使用的广度和深度的模型，以及自研的去噪自动编码系统。和传统的推荐模型相比，深度学习技术可以更好的理解用户的需求和给出更高质量的推荐结果。利用此技术，再加上由 **Box Unpac**k 所提供的区块链开发库，开发人员可以为 ContentBox 平台上的每一位用户构建出一个前所未有的推荐引擎。

一键解决方案

除了上述提到的开发者工具，**BOX Unpack** 还为那些想要为用户提供数字内容服务，但却受制于资本和技术的初创公司提供了简单的一键解决方案，帮助他们创建全功能的在线平台。想象一下，当一个小团队想要用他们刚刚创建好的优秀播放器来搭建一个更好的视频 APP 的时候，他们的第一个挑战就是高额的版权成本。有了这个解决方案，团队即可通过创建一个收入共享计划的方式，无需编写任何智能合约，就可以轻松克服上述的版权障碍。我们有理由相信，这个一键解决方案将会大幅降低合作伙伴使用 ContentBox 来进行开发和增长的门槛。

相关工作

目前有太多的项目正致力于解决可扩展性和当前区块链的隐私问题。不幸的是，它们都无法被直接应用来克服特殊的挑战，而这却正是 ContentBox 所致力于要解决的问题。尽管如此，它们本身还有许多潜在的，可以被借鉴的技术，我们会积极的监测它们的进展。

Sharding

与传统数据库软件系统（如：MySQL）类似，区块链上的分片是一种提高系统整体吞吐量的手段。其核心理念在于拆分整链为不同的‘片’，每片仅并行处理整体的一小部分。
许多区块链开发者视分片技术为解决可扩展性问题的一种有发展前景的办法。也有不少的区块链项目将此方案作为他们的技术底层。但是，当谈及不久之后就能上线的主网，我们对其能否在主网上全面安全的实现仍持保守态度。基本地，‘分片’这一区块链技术想要创造一种网络，在这个网络中，每个节点只处理所有交易的一小部分，同时仍然保持较高的安全性。找到一种快速且安全的办法来解决扩容问题仍非一日之功因为在区块链上所执行交易可以依赖于区块链里的前一次状态的任何部分，这使得并行处理变得更加困难。而‘片’之间的消息传递则变得更加复杂。总的来说，我们认为分片技术仍需要经过一个漫长的发展之后才能成为一个广泛接受的区块链扩容的解决方案。我们将密切关注这一领域的进展，但不会将其作为我们目前解决方案的核心技术。

[8] https://github.com/ethereum/wiki/wiki/Sharding-FAQ

闪电网络和雷电网络

基本而言，所有的这些闪电和雷电网络依赖于链下状态通道。这里的核心思想是参与者将一些比特币或以太币放入一个多签名的地址，开放一个支付渠道，然后在不提交区块链的情况下签署交易。任何时候，任何一方都可以关闭支付渠道，而最后所签署的交易，即双方最新的余额，都将会被提交给区块链。
如果可以应用良好，这两种方法可以在各自的环境中提高交易吞吐量和降低费用。（一个用于比特币，另一个用于以太坊）。但是，在实际情况中仍有一些限制。例如，一笔交易里所有的参与者需要在通道关闭之前锁定一些 token，这样就降低了支付网络的实用性。

Plasma

Plasma 是在区块链上扩展智能合约计算的最具前景的方案之一。在 Plasma 中，区块链由树层次结构所组成，每一个分支都被视为一个区块链，它有自己的历史和计算记录，这些都是可映射的。因此，根链只需要处理来自子链的少量的 Merkel 证明，这将促使更高扩展性的出现。

提出 Plasma 的两位作者都是区块链领域的大师，他们提出了一种全新的解决方案来解决目前区块链网络的长期问题。理想情况下，它将适用于数字内容产业，并可以作为 ContentBox 的基础。但是，该项目还处于起步阶段，一些重要的问题亟待解决，例如如何抵御在子链上发生的攻击。在 Plasma 论文里写到的，关于将参与者转移到另一链上的解决方案远非完美，因为并不容易实现和保证资金的无阻流通。他们的整个智能合约系统仍然容易受到潜在的安全漏洞的威胁。
因此，我们认为 Plasma 是一个改进和升级过的以太坊，它仍然需要一定时间来展示具体水平和能力，所以我们不会选择将它作为 ContentBox 的技术基础。

MimbleWimble

MimbleWimble[12]大约是一年半前提出的一种新的区块链设计。

[9]https://lightning.network/
[10]https://raiden.network/
[11]http://plasma.io/
[12]https://github.com/mimblewimble/grin

与目前的主流区块链系统相比，它理论上可以提高区块链的隐私性、可扩展性和可互换性。
它的核心思想在于人们无需下载所有的交易数据即可验证系统的状态。相反，该链可以高效的压缩交易历史，并依赖于密码基元来实现完全的公共可验证性(这与我们的解决方案非常相似)。此项目最近取得重大突破，推出了测试网络并集成了 Bulletproofs。
但是一个完整的 MimbleWimble 节点仍然需要大量的磁盘空间，这使得它对移动设备不友好。并且按理说，剥离比特币脚本系统的设计将使其难以分叉，并削弱其在支付方面的能力，而这在数字内容产业中是非常重要的。尽管如此，MimbleWimble 仍是针对区块链扩容问题的一个很有前途的解决方案，我们可以从其设计和应用得到很多灵感。例如交易的结构，用于压缩区块的通路以及自带的鼓励去中心化挖矿的抗 ASIC 挖矿算法（Cuckoo Cycle）。

Steem

Steem 是一个用于生产智能媒体令牌的区块链，它促进了去中心化的博客和社交网络的出现: Steemit[15]. 通过设计，Steem 利用委托权益证明（DPoS）共识机制来实现高吞吐量。此外，它还引入了一些创新的内置功能，如奖励池、链基，以及以股权为基础的投票和激励机制来支持 Steemit 的运营。
一般来说，Steem 是一个设计良好的社交媒体区块链平台，具有出色的性能和丰富的内置功能。但是，从基础设施的角度而言，Steem 过于以应用为导向。在支持 Steemit 运营的同时，奖励和投票系统也同样限制了除社交博客以外的其他应用程序的使用。例如，一款移动视频 APP 可能不需要投票行为来确定用户对某一条视频的兴趣；他们可以通过简单的观察用户行为来学习，比如浏览，查看，暂停，快进等。实际上，很多初创公司利用用户的行为数据和先进的人工智能算法来管理和分发个性化内容。
Steem 的基础设计开起来令人印象深刻，但却未必适合 Box 的核心系统。相反，我们更倾向于将区块链作为整个系统的微内核，并将打赏或投票功能限制在应用程序级别，以提高灵活性。我们的架构无疑是用来开发开源生态系统的更好方式，它为数字内容产业的 ContentBox 的采用奠定了基础。

[13]https://www.coindesk.com/magical-realism-mimblewimble-just-launched-first-testnet/
[14]http://web.stanford.edu/~buenz/pubs/bulletproofs.pdf
[15]https://steemit.com/

与Castbox App的集成

移动钱包

一个轻量级的钱包将会被集成在 Castbox 应用里。当一名用户使用 APP 的时候，通过内置钱包，他可以快速查看账户余额和转账记录。未来，这个钱包将会显示跨 APP 之间的余额。

作为一个流行的移动 APP，Castbox 是一个 BOX token 移动钱包的逻辑宿主。通过第一时间让 Castbox 上的数百万用户登录并创建一个即时在线的生态系统，ContentBox 将会避免大多数初创公链上线时无人问津的尴尬处境。 除此之外，因为 Castbox 是一个用户经常使用的 APP， 大部分用户在一天之中会很自然地与 ContentBox 进行多次交互并逐渐建立起加密货币相关的概念。 长期来看，当用户在使用 BOX token 的过程中有良好的使用体验，并在全新的区块链系统之内收益颇丰的时候，他们便会促进其他基于 ContentBox 开发的应用程序的出现，从而增加和扩展社区生态里的用户数量。

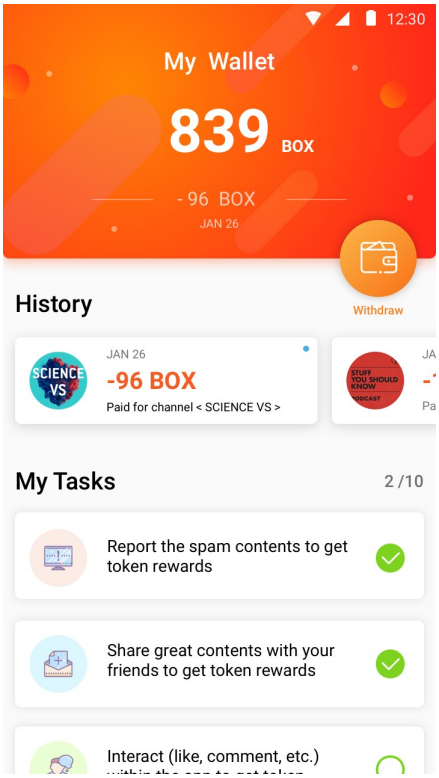

图 6: APP内置的轻钱包

BOX Login

Box Passport 系统上线的时候，Castbox 将会把合规的帐户迁移到区块链体系中中，并给予用户一个安全通用的 BOX ID。 待到迁移完成之时，Castbox 的后端服务器将不再存储用户的帐户和证书信息。取而代之的是，App 的客户端将会在用户登入的过程中接入区块链系统来检索并验证用户的身份。

使用 **Box Passport** 不仅让终端用户受益良多，也会给 Castbox 的运营方带来诸多益处。鉴于验证和授权的重任已从 App 的服务器转交给了公链，运营方也不用再承担为保护用户信息防止黑客入

侵的高额人力成本。另一方面，用户也可以取得对自己数据的控制权，从而降低了个人信息泄漏的风险。

基于BOX token的应用内奖赏系统

除了轻量级钱包，一个 token 奖励系统也会一起被嵌入 Castbox 中。 这个奖励系统主要包含两个目标: 用物质手段激励作者创作出更多有价值的内容以及鼓励用户管理和传播优质内容。例如，一名听众在 Castbox 发现了一个有趣的播客，写下评论然后分享给社交网络里的朋友（例如脸书和推特），作为回报，他将会收到一些 BOX Token。

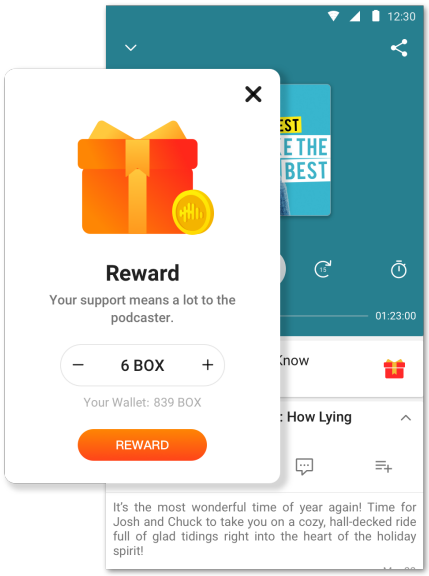

图 7: 通过举报刷屏来挣取BOX

用户也可以帮助过滤刷屏来获得 token。 水军对于每一个网络社区都是一个挑战，如果不能得到有效控制，将会大幅降低用户体验。 通常情况下数字内容平台解决此类问题的手段就是通过雇佣大量的监管员或者投资开发和部署 AI 人工智能算法来自动过滤水贴。但是所有的这些办法不仅低效并且成本高昂。通过内置的激励系统，Castbox 的用户就会主动举报无用内容来获得奖励。

除了Castbox，还能衍生出什么样的DAPP？

当开发者使用 BOX Unpack 和 BOX Passport 时，更多新的应用将会在 ContentBox 平台上被创造出来并成功部署，ContentBox 作为数字内容开源社区将会带来更多可能性的应用实例。下面是几个概念层面的例子：

去中间商的内容交易市场

现如今，内容发布被集中在几个中心化的应用市场，如 iTunes 和谷歌商店。 这些平台单方面的决定了创造者可以拿到多少报酬。结果就是，全球的大多数创作者创造的财富和他们拿到的报酬是不对等的，有些甚至拿不到报酬。而 ContentBox 则是一个开放的，公平的，以创作者为中心的去中心化应用平台。如此设计将会比中心化市场带来更多的优点：

- **更低的交易成本**：因为减少了创作者和消费者之间数字内容发行平台，省去大量的中间环节的克扣，创作者会获得更多的利润。
- **更高的流动性：**例如在音乐产业里，一首歌曲被制作出来后，经常得花上六到八个月，作者才能拿到版税。在我们全新的数字商店里, 只要一名作者的歌曲被全世界的任何一个角落所下载，那么他就立刻能获取 token，可直接在交易所兑换成所需货币。
- **更高的透明度**：因为所有的重要信息都被公网所登记在案, 一名作者可以清楚的知道自己的歌曲被下载了多少次，可以产生多少收益，保证利益不会被大平台克扣。

小额众筹站

传统情况下，很多内容创造者几乎找不到愿意资助他们的创意项目的途径，只能依附于强大的媒体经纪公司，如音乐发行公司和电影发行商，只有个别的项目会得到这些公司的投资和包装，而更多有才华的人被挡在门外。 而在 ContentBox 上，创作者们就可以独立募资了。一名电影制片人可以向粉丝预售 token 用来给独立电影募资，一旦电影制作完成，就可以保证粉丝享有电影的尝鲜权甚至股权。 众筹智能合约也带来了几个更高级的功能，例如，粉丝可以按照他们所持 token 的比例来享受电影盈利后的分红。或者以产品所到达的不同阶段，分批次逐渐释放收益给前期投资的粉丝。 相同的做法也可以应用到其它形式的内容产品，如音乐和 TV Shows。

基于 ContentBox 生态系统的众筹平台可以利用已有的大量基础用户，就像目前其他的众筹平台一样。 而 ContentBox 上的数字货币可以无缝接入到这些众筹活动，免去了发起众筹活动的额外现金支出。

去中心化“AdSense”（谷歌广告联盟）内容广告平台

AdSense 是谷歌的广告联盟，允许谷歌内容的网站发布者投放自动文本或者多媒体广告，旨在将特定内容推送给特定受众。在 ContentBox 平台上也同样可以有类似计划来促进广告商和内容出版人之间的交易。 和谷歌广告联盟有所区别的是，这一切是基于区块链而非谷歌这样的巨型中心化平台。 广告目录可以借由类似 IPFS（ 文件系统）这样的去中心化目录系统来管理并且可以利用基于 **BOX Unpack** 提供的模块来开发调度引擎。货币化和支付同样可以用过 **BOX Payout** 来完成。

和谷歌 AdSense 相比较而言，这种去中心化的广告计划可以提供更透明和更可靠的服务。没有了中心化的权力傲慢，各方享有更多的灵活性：广告商的支出下降了，出版人的腰包也更鼓了。

跨平台的新型媒体播放器

通常情况下，一款媒体播放器只是能够解码多种多媒体格式的电脑端或移动端软件。 但是，在ContentBox 平台上可以衍生出一款全新的播放器。除了播放用户设备里的视频剪辑之外，这种全新播放器还能够让用户搜索 ContentBox 平台里注册在案的各种视频或电影，尽管这些视频可能会被托管在不同的 ContentBox 合作者使用的服务器上。通过流媒体的形式，在播放过程中，播放器会实时、自动地收集 BOX token，并将这些币发给对应的版权拥有者。

这款播放器的底层技术就是可以和我们的 ***BOX Payout*** 和 ***BOX Passport*** 进行交互。有了ContentBox 的帮助, 播放器就可以在这个拥有海量版权明晰的内容共享池里进行挖掘并且极大提高用户的视频点播体验。如果没有 ContentBox 这两个关键技术支持，那么这种创新型播放器也就不可能落地了。

规划图：

Castbox 和 ContentBox 的技术规划如以下时间表所示：

- 2016.01 Castbox 团队建立
- 2016.02 Castbox 上线安卓平台
- 2017.01 Castbox 上线 IOS 平台
- 2017.10 Deep in-audio search 功能上线
- 2018.03 Token 交易
- 2018.09 Token 整合至 Castbox app 里（已完成）
- 2018.12 *BOX Passport* 完成（Alpha 版本）
- 2019.03 进行 *BOX Payout* 上线测试
- 2019 Q4 *BOX Payout* 主网上线

Token分发

ContentBox平台上的数字加密货币（**BOX Token**）是经济生态的重要组成部分，并且被设计为平台上唯一流通的货币。在**ContentBox**平台的原生区块链系统（主网）正式上线之前，**BOX** 币将先以ERC-20以太坊Token标准的形式发行。一旦BOX 的主网上线并且运行稳定，这些ERC-20 token将会以1：1的比例进行映射。

份额

总发币额：30亿
BOX

百分比	用途	详情
25%	预售	针对机构投资者, 锁仓时间最高为 6 个月
15%	团队持有	奖励内部的研究与开发团队和开源社区的志愿者，分四年发放
30%	社区生态里的奖励	奖励所有的社区生态的参与者，比如创作者，听众，私人投资者和平台等
20%	基金会	保障 BOX 币免于投机炒作并为基金会的运作提供资金
10%	合伙人	为赏金计划提供资金以及与其他音频/视频网站或 APP 建立良好的合作关系

所得款项用途

比例	项目
50%	研究和开发
25%	营销和推广
15%	用于法务，审计和合规性事务
10%	一般事务和行政开销

团队成员

•王小雨 ReneeWang -CastBox 的创始人兼 CEO，本科毕业于北京大学。Renee 于 2016 年开发了 CastBox，并在过去的两年里带领公司迅猛发展。在这段时期里，她不仅仅缔造了一支近 50 人的国际化的队伍并且斩获接近 3000 万美元的融资。 Renee 曾供职于谷歌北京，谷歌爱尔兰，谷歌日本。 她是友盟的第七名雇员，也是一名安卓工程师。友盟——中国最专业、最有数据凝聚力的移动开发者服务平台，后被阿里巴巴收购。早在 2008 年，她就是最早的安卓开发者之一了。

- **胡钢 Hu Gang** -首席密码专家兼 ContentBox CTO.**胡钢**是一名连续创业者, 系统构架师以及拥有数十年网页和移动 APP 开发经验的全端开发者。2002 年毕业于北京大学，获计算机科学硕士学位。于杜克大学取得 MBA 学位。 他是 5MILES 的合伙人兼 CTO。5Miles——一个处于领先地位的，拥有全美百万日活用户的电商平台。

- **贺晓聪 Alex He** - 1999 年毕业于北京大学。CastBox 的联合创始人兼 CTO. 自 2003 年到 2015 年, **Alex He** 曾供职于摩托罗拉，播思和小米。热爱 Linux/Java/安卓移动软件的研究与开发。自 2007 以来, 他就已经从事了安卓移动技术的研究和开发，并且也是早期的安卓开发者之一。**Alex He** 从北京大学毕业后就加入了 founder institute，致力于多媒体领域的软件开发和研究。 **Alex He** 所参加的研究和开发团队数以百计。并且他还是一名在 GitHub 上非常活跃的开源开发者。

- **刘晓晖 Dr. Xiaohui Liu** - 区块链科学家，FaceBook 前科学家。设计并部署了针对下一代的网状网络的分布式协议。刘博士在分布式网络协议拥有十年的研究开发经验。 他在世界软件工程师协会（ICSE）拥有 1 项专利，发表过 9 篇论文.他在中国武汉大学取得了学士学位，于美国韦恩州立大学取得分布式网络博士学位。
- **戴方勤 Fangqin Dai** - 任技术主管。 谷歌前高级软件工程师。开发了矿池软件并用超过 1000 个 GPU 挖掘 ETH，他在智能合约的发展进程中可谓是如鱼得水。**方勤**曾供职于一些顶级公司如百度，英特尔，淘宝和金山，有着 7 年的行业经验。在 GitHub 上，他有 2400+ 的粉丝，并且贡献了数不胜数的流行项目代码如 Apache Spark 等。**方勤**本科毕业于武汉大学，获清华大学硕士学位。

- **王一强 Yiqiang Wang**-开通金融的创始人，前 CTO。开通金融——成立于 2015 年的金融科技公司。直到 2018 年，开通金融服务了上百家大中型互联网平台和金融机构，总交易额超过 1 亿人民币。加入开通金融之前，一强就职于友盟技术部门，曾任友盟移动统计分析业务技术总监。友盟为国内移动应用的开发商提供类似数据分析等服务。**一强**毕业于复旦大学，获计算机科学学士，硕士。

风险：

您已知晓并承认购买 BOX 币，持有 BOX 币以及在 ContentBox 平台上存在风险。

不确定的法律法规和监管措施

针对 BOX 和分布式记账技术的法律法规在许多地区还尚不明确。也不可能预测到监管机构何时或是否会运用现有法规，或就此类技术及其应用的出现，包括 BOX 和 ContentBox 平台而制定新的法规。监管措施可能在不同的情况下对 BOX/ContentBox 起到负面影响。 基金会 (或其附属机构) 在监管行为，法律法规发生变化的情况下，在司法管辖范围内，或出于商业目的必须要取得相应批准方可此类管辖范围内运作，可停止在管辖范围内的业务。

咨询过大部分不同领域的法律顾问并对虚拟货币的发展和法律结构进行持续的研究之后，基金会对 BOX 币的发售持审慎态度。因此，对于众筹，基金会将会不断调整销售策略以尽可能避免相关的法律风险。对于众筹，基金会和 **Tzedek law llc** 一同合作。**Tzedek Law LLC** 是一家在区块链领域拥有良好声誉并经验丰富的新加坡律师事务所。

竞争者

可能会出现利用 BOX 和 ContentBox 平台的底层代码或类似协议的变种网络来试图抄袭类似功能。ContentBox 平台就不得不去与这些变种网络竞争，而这对 BOX/ContentBox 平台来说是不利的。

人才的流失

ContentBox 平台的发展离不开目前技术团队和专业顾问的持续合作。他们在各自的领域都经验丰富，有所建树。失去任何一个成员都会对 ContentBox 平台的未来发展都有负面影响。

开发失败

ContentBox 平台存在开发或实施不如预期的风险。基于各种原因， 包括但不仅限于发生数字资产包括虚拟货币或 BOX 币价格下跌的情况,以及不可预见的技术困难,以及用于各项开发的资金匮乏。

安全漏洞

黑客和其他恶意团体或组织可能会尝试用多种方式攻击 BOX/ContentBox 平台，包括但不仅限于勒索软件攻击，阻断服务攻击（DOS），共识攻击（51%攻击），女巫攻击，smurfing 攻击。除

此之外，还有第三方或基金会的成员或其附属机构有意或无意泄露 BOX/ContentBox 平台核心架构的风险。

其他风险

除了上述提及的风险，在您购买、持有和使用 BOX 的过程中，可能会还有其它的风险，包括那些基金会无法预料到的突发情况。这些风险可能会演变为预料之外的风险或者是上述提及的风险的组合。在购买 BOX 之前，您应该对基金会（及其附属机构）、ContentBox 团队进行全面的尽职调查，了解关于 ContentBox 平台的总体框架和愿景。