ABC -反官僚代币

使用区块链以便于分散身份，签名和文档的真实性的数字平台

爱迪尔逊·欧所里·祖妮尔, 米立安·托米埃·欧世罗,何雷娜·苏勒兹·马佳利多

OriginalMy.com

7月, 2017

草案 v1.2

1. 摘要

自2015年以来，我们开发了一个平台，我们以块分散的方式提供新的应用程序，重点是以分散的方式生成记录和强大的真实证明。

已经是使用块链接到现实世界案例的第一个regtech，我们在巴西用户已经可以使用的应用程序除了提高效率，降低成本（例如纸张的非物质化，运输和真实性的识别）传统机构的手动模式），并将任何负责注册的中心组件过时，并对某些内容的真实性进行认证。

巴西在“经济自由指数”中处于第140位[1]，在国际上受到阻碍该国业务发展的大型官僚机构的承认。他们是正式的官僚机构，并承载所有民法国家的利润丰厚的业务，其中包括拉丁美洲和欧洲的大部分地区。然而，信息的集中化是一个全球性的问题，信息上的不对称最终使得人们和组织更容易受到欺诈的侵害。

改善这些不对称性的主要关键是权力下放的真实性，这可以通过使用公共块链的分散式架构来实现，从而提供访问和信任，并具有完全的透明度。

在本文中，我们介绍：
- 活动应用程序，正在运行的应用程序及其规格
- 新平台
- ABC代币 - 反官僚代币

2. 目录

3. 词汇表

为此，采用了一些定义，使得以大写字母开头的字和/或术语，包括名义一致性的功能变化，应具有以下列出的含义。

- 数字签名：验证数字文件或信息的加密方法，这明确证明原始信息没有遭受任何类型的更改。
- 电子签名：使用任何电子机制进行签名，不一定是密码方式。它作为证明的指示，本身没有合法价值，相当于物理介质上的签名。
- 真实性：表示某物的绝对有效性，准确性和/或独创性。确定某些信息来自指示的来源，并且它是满的，即不是修改的目标。
- 区块链ID：由OriginalMy创建的分散式公共块链中注册和管理身份的方法，允许用户验证用户，而不保管文档或私人和/或机密信息。
- 民法：也被称为守则法，是世界上传播最广泛的法律制度。它以罗马法为基础，通过法律编纂系统化。在这些制度中，法律的主要来源是书面法（积极的）。
- 普通法：盎格鲁撒克逊起源的法律制度，其中用法和习俗的主要法律依据以及司法机构（案例法）已经判断的先例。
- RPP：由巴西联邦税务局颁发的身体登记。这是纳税人和居住在巴西的个人人数。
- 公信力：由公权力选出的人员颁发的文件和证明书提供的真实性的法定推定（juris tantum）。
- 电子文件管理：电子文件管理。这是一种技术，可以轻松创建，管理，存储，共享和检索文档中的现有信息。
- 信息：可以存储和/或转让任何对个人和/或组织具有重要意义的内容。
- KYC：了解您的客户的简介，是识别和验证客户身份的过程。它们是受规管市场，特别是金融和资本市场参与者所需的流程，旨在遏制洗钱，腐败和恐怖主义等非法利益非法行为的做法。
- 喷气洗涤作业：巴西联邦警察局进行的一系列仍在进行中的腐败，欺诈，洗钱，犯罪组织，资本外逃等罪行的调查工作。迄今为止，已有282人被起诉，107人被判刑[2]，其中包括政治家，公务员和私人行政人员。公共资金的估计损失约为420亿新元[3]（134.2亿美元）。
- OTC 市场OriginalMy：根据白皮书中规定的规则，由OriginalMy提供的柜台市场将直接由基于二级市场价值的公司购买和销售ABC代币。
- 固定链接：URL直接指向具有多个帖子（博客，社交网络等）的网站上的特定帖子。
- OriginalMy平台：由OriginalMy开发和提供的应用程序集，基于记录的概念和块中的真实性证明。目前，它由以下组成：（i）块链ID，（ii）数字文档的真实性证明，（

iii）网页内容的真实性证明和（iv）文件和合同的数字签名。可访问 https://www.originalmy.com。

- 工作证明：使用复杂的加密计算来防止大规模网络攻击的协议。在其中，用户在执行所需的操作之前执行一定的任务，向验证者证明使用自我努力，然后接受访问或主动作。
- 真实证明：某些数字文件具有真实性的证据。
- PTAX：根据3.13：1计算，2017年10月4日基准日的Real兑美元的官方兑换率[4]。
- 真实记录：是数字签名在任何媒体中的存储。
- 路线图：按照具体规定，OriginalMy的发展目标达到人群第一阶段的目标。
- 信息安全：涉及保护信息，目的是保护其机密性，完整性，可用性，真实性和合法性，如ISO / IEC 27000标准
- 边链：大致是批处理来自其他块链的数据的块链，而不需要修改后者的原始代码。可以协助本地协议的可扩展性，效率和成本的问题。
- 法律制度：具有法律保障目标的法律模式。 寻求这一结果的方式解释了构成它们的不同法律制度和制度的运作。 目前，世界上主要的制度是民法和普通法制度。
- 网络信任：使用加密级别和链接建议的声誉系统，以加强对不同代理商的信心。

4. 概念

4.1基于区块链的信息和技术的安全性

信息安全的最佳做法是保护，使用和访问信息，以及其对用户的可用性，同时其完整性和真实性仍然保留，并根据适当访问的控制使内容暴露。

信息安全的主要特征[5]，一些在以前的ISO / IEC 17799（灵感来自标准BS 7799）中，后来在27000年的一系列标准中进行了审查：

- **保密性**：确保只有获得授权的人员才能访问信息;
- **诚信**：保障信息和处理方法的准确性和完整性;
- **可用性**：确保授权用户在必要时可以访问信息和相应的资产;
- **真实性**：确保通信过程中的信息和/或用户是他们所声称的;和
- **合法性**（或合规性）：是通信过程中信息的合法价值。

然而，根据一些作者，信息安全也是不可否认的或不可逆转的，这是确保在通信过程中**不可能否认作者身份**的属性。

基于区块链的技术通常遵循信息安全的属性，如下所示：

1. **信息安全属性的三位一体**是公共块链协议中本质的，即仅通过识别交易所必需的数据来保证机密性，仍然存在一些保密匿名的块链协议交易。通过协商一致确保数据的完整性，主要通过工作证明（工作证明）。通过网络的分散和分配实现可用性，酌情促进业务连续性计划的可能性;

2. **通过非对称加密技术**，使用数字签名和通过私有权授权的私钥来保护信息的真实性;

3. **合法性**是从上述项目的预测符合规定的框架和法律，为信息和数字文件提供适当的处理。

这些技术仍然是不可侵犯的，其验证机制一直被使用，可以简单的方式验证，并确保信息的完整性[6]。

4.2 功能障碍的官僚主义

在广义上，官僚主义可以被定义为一个按照预先确定的严格规则运作的组织，以确保"*精确，速度，确定性，档案知识，连续性，严格从属，减少分歧和物质成本和人*"[7]。这个概念是理解社会，国家和现代资本主义公司等复杂组织形式的基础，因为通过严格的规则制定秩序，控制和确保执行这些机构的职能的效率。

因此，官僚主义是假设特征，如果适用于复杂的组织，将产生功能类别：理性，标准化，层次，专业化和不人性化[8]。
事实上，如果在这方面，官僚作风对于创造复杂而有效率的组织来说可能是决定性的，另一方面可以导致这些组织的权力集中，导致系统性障碍，在极端情况下，可以是抹灰系统有利于现状的持续存在，损害公共利益。

这方面的一个例子是巴西，滥用僵硬的规则导致了官僚机构不正常的象征，在处理公共政策和执行非法行为方面无效。这是真的，自2014年以来，已经对历史上已经报道的最大的腐败案例进行了研究[9]，被称为"喷射洗涤作业"，仍然没有得出结论。

在巴西的这个体制危机之中，OriginalMy诞生了，目的是消除文化和社会沉重的功能失调的官僚主义，这不仅对允许腐败和洗钱的案件负责，因为它也是促进社会进步的主要限制因素和行使自由主义。

但巴西不仅遇到这个问题，在所有民法国家，我们可以找到公共和私人的机构，他们从公信力的寡头垄断中获利，建立消费流程，没有直观的信息获取和真实性检查。在实践中，真实性证明的集中化是信息不对称的主要来源之一，不仅打破了市场效率低下的空间，而且开辟了欺诈行为的实践。

在其他国家，特别是基于普通法的国家，真实性证明的集中化通常是基于对信息有任何权利的个人或组织，可能的虚假和/或不准确的处罚方式，例如欺诈和欺诈性虚假陈述等机构。然而，通过集中化，虚假的证明就是一个准恶魔的证明，即使是多个传票也可以解决。因此，与民法相同的方式，不可能评估信息的真实性对企业和社会造成巨大损失。

那么，真实证据的集中化，无论是在实证主义国家还是那些利用海关作为主要法律依据的国家，都是支持官僚机构功能失调的重要支柱。最大的证据在于，在这个过程中最常见的后果（贿赂，游说和欺诈）由各国个人，组织和政府每天面对。

因此，世界陷入恶性循环，因为如果一方面实行正式的官僚制度来阻止非法做法，另一方面则鼓励集中核查信息。因此，三合会意志机会，允许个人和组织有权谎言和作弊保持不变，这可以导致结论，强加的官僚主义的这些新的“层次”与目前的管理体系有同样的缺陷真实性的信息和测量。因此，预期结果再次是功能障碍。

在完全相反的范围内，是利用公共和分散式块链的技术：其中，通过支持协议，人们参与的激励大于尝试欺诈的动机[10]。此外，非常分散化使得只有一个人或组织不可能集中所有必要的特征来欺骗某些信息（愿望，能力和机会）或不当使用它。

分散形式的信息真实性的注册和计量可能导致在某些信息的所有者和利益相关者之间分配公信力，使公司和全球社会无法估量的收益。

4.3 权力下放记录和真实性

由区块链协议保证的信息安全属性的上三位一体，真实性和合法性的属性仍然依赖外部应用程序来遵守各种监管框架和现有法律，完成所有意图和目的的预测形式，可以反映完美的法律行为。
在这个意义上，OriginalMy平台通过使用各种公共块链来提供文档和信息的分散真实性。这与其他开放协议相结合，有助于为身份创建真实性证明，表达自主权（作为条目，访问和签名文档的用户登录）以及各种数字文档。

在实践中，有可能采取所有法律要求的存在，有效性和有效性，包括真实身份验证的行为，包括法律业务的庆祝，不仅拥有一个密钥或密码。

真实信息是可以验证其原始状态，并且没有对其完整性进行任何更改。对原始信息使用复杂的加密算法，可以以某种方式找到代表它的新信息。给这个新信息给出加密哈希的名称，由一定数量的字符序列表示（像这样一个：
c66663acfe3611b9ed95c79aad41dc6fca836363680 7cfd4ee7b88ef15fa34）。这个哈希是该信息的真实性证明。

意识到通过*哈希*不可能推断信息是什么，甚至不能重建它。只有在原始信息上应用相同的加密算法才能进行真实性验证。如果它是真实的，将显示相同的哈希。将原始信息的*哈希*与验证的信息进行比较，可以确定第一次遭受的修改，因为在任何更改的情况下，生成的*哈希*将不同。

为了确保没有人替换或更改原始信息的哈希值，OriginalMy将其注册到一个或多个公共块链中，而这些公钥块现在存储它。一旦块链确认到存储器，它提供代表它现在拥有该特定散列的时刻的时间戳（*时间戳*）。这是真实性证明，某些信息以某种方式与验证的信息以相同的方式存在。而且，在此确认之后，此真实性证明将自动复制到组成每个块链的网络的所有结点，其中注册的制作。

鉴于公共块链的基本特征，如不变性，透明度，权力下放和数据分发，OriginalMy为数字文档提供了分散的真实性，而无需记录或公开用户信息的内容，保持他/她的隐私和保密。

模式和开放式协议的模式往往比封闭模式更有效，因为它们是可审计的，并且有专门的社区来发展。

因此，OriginalMy使用可以被其他智能合同系统公开访问的几个dApps [11]（分散式应用程序），共享基础设施以提高流程和控制的效率。

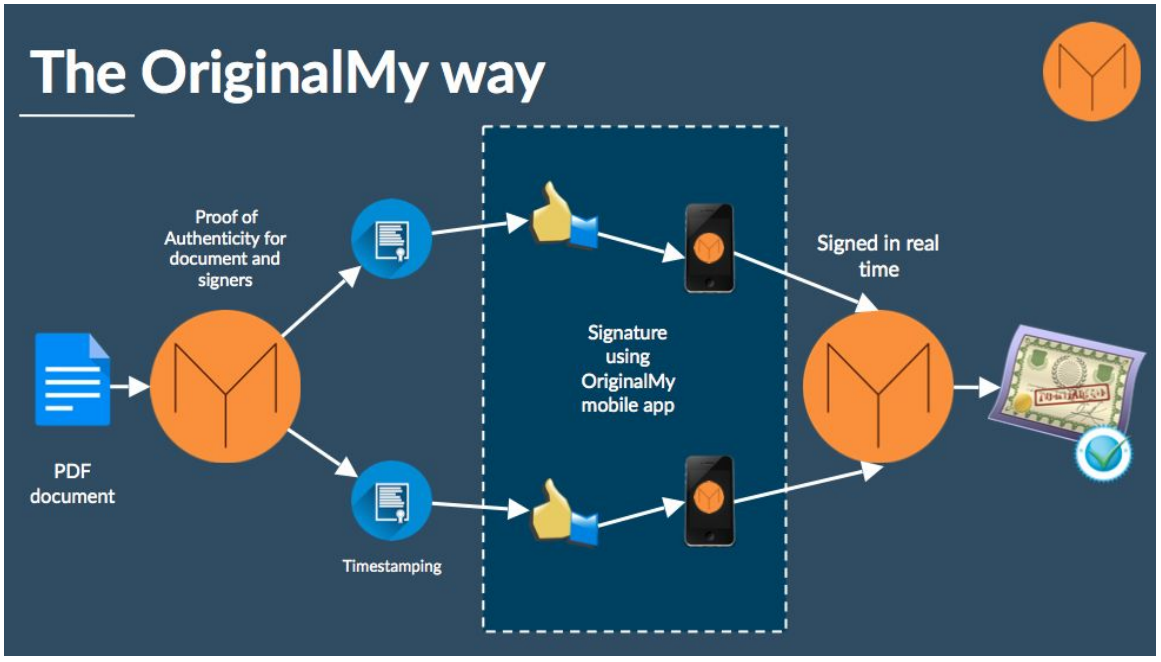


图1：使用OriginalMy平台的示例：使用身份验证签署文件和合同。

5. 实际平台应用及历史

5.1 真实性证明

OriginalMy平台于2015年7月18日在巴西弗洛里亚诺波利斯举行的III Bitconf活动期间推出。在那一刻，平台正在使用数字文档的真实性证明的方式进行记录，利用文档的数字签名和比特币网络提供的时间戳。

5.2 合同签名 - 第1版（已停产）

发布后不久，我们核实了将签名解决方案的要求提交给封锁注册文件（即就其内容提供同意或一致性）。在分析哪些是现有数字和/或电子签名媒介的主要法律挑战时，我们得出结论，数字环境的大问题是验证，实际上是这样做的人就是表达意愿的人。

特别是关于这个话题，值得一提的是，即使使用块链开发的传统技术解决方案从您拥有密码或密钥开始就足以验证您的身份。然而，这种推定已经被证明是无效的，以确保真实性，特别是当您注意到数字媒体中的新奇数量的欺诈（黑客，恶意软件或简单的“白色欺诈[12]”），以及常规行业不愿意将记录和验证迁移到完整的数字环境。

解决这个问题的第一个办法也是在2015年，当时我们通过视频证明开发了第一版的文件和合同签名系统。在此，我们可以应用生物识别验证来检测和评估几个控制点，作为表达中的说话，微观表达等的压力水平。

然而，尽管从法律的角度来看，这种模式没有获得预期的遵守，因为它带来了重要的转型成本：人们习惯于签署文件，而不是通过视频来声明它们是的内容。

因此，我们开始研究和开发一种具有相同法律后果的新型电子签名系统，但具有更好的可用性和用户友好性。我们了解到，电子签名不是针对问题的目标，而是关于其作者的身份，所以与用户抵触欺诈的层面有必要。

在2016年初，我们开始制定一个新的模式，同时可以通过身份认证来证明完美的法律行为的真实性，而不是用户的竞争，用于签署文件和合同，并减少在以前的视频证明模式中验证了摩擦。

此签名模型已更新为新的，用户友好和更好的模型，仅供遗留模型咨询。

5.3 幕达莫斯+ 项目

一旦我们制定了协议，ITS-Rio（里约热内卢理工学院）就邀请我们制作出可以促进“人民行动法律项目”签名的解决方案[13]。

使用由OriginalMy开发的用户和签名的新识别模型，ITS-Rio于2016年被授予Google.org的社会影响挑战奖[14]。因此，我们基于我们设计的协议的定制版本，使用块链开发了所有层的身份和签名。

特别是对于Mudamos + [15]，我们开发了一个专用于注册公民签名的Sidechain，并在公共块链中进行验证。这些签名来自移动应用程序Mudamos，其使得用户的KYC发出保持存储在移动设备中的块状标识。

然而，为了增加安全性并降低欺诈风险，应用程序在用户自己的设备中执行每个签名的工作证明（生成一个单独的交易块）。这种工作证明是基于hascash算法[16]，与Bitcoin一样用于验证交易并避免欺诈。

迄今为止，Mudamos +已经拥有超过27万个独特的注册用户，50万次下载和使用由OriginalMy开发的定制引擎的24万个签名，巴西的几个联邦机构接受了与此应用程序签署的法律项目。

5.4 网页内容的真实性证明

在第一次应用程序中的几次演示之后，我们向我们介绍了在块链上收集真实Web内容的证明的需要，以及自动时间戳。例如，所收集的内容可能来自于社交网络的非法行为，并且可以在司法行为中使用证明来验证在该特定时刻某些内容在因特网上可用。

因此，我们开发了一个Chrome插件，用于收集当时观看的内容（最好是通过“永久链接”），生成使用文档证明所必需的司法理由的报告，并将收集的内容注册到一个区块中。

5.5区块链ID：记录和管理身份

幕达莫斯+项目的定制版本，我们的记录方法和身份管理（“区块链ID”）的方法证明了一些用户是他所声称的用户，以及他所声称的所有行为（作者真实性）通过我们的平台

我们在2016年4月发起了这个协议[17]的开发，使用当前电子签名模型缺乏可靠性的场所，以及根据几个国家的监管框架来衡量身份真实性的要求，以及几个现有协议的参考，其中一个是比特ID [18]

最初创建了区块链ID，以便合同和文件的签名可以形成由存在，有效性和有效性包围的司法业务，包括如何在最近的电子签名系统的弱点，无法保证和证明作者身份。

通过区块链ID开发并提供的注册和身份管理方法已经显示出非常有效，即使可以对其进行一些重要改进（进一步解释），我们开始将其用作数字KYC的一种方式，允许用户不再需要密码和密码来访问网站或填写表单。

关于使用块链的身份系统和KYC的主张的主要新功能，至今存在于市场上，我们可以列出：

1) 希望对身份记录没有任何成本。因此，网络的入口对所有希望获得区块链 ID的用户将是免费的;
2) 根据第三方的身份是一项人权，并不得因任何其他人的授权或补救而不得受权力或侵犯;
3) 使用生物测定法来访问或做出明智的行为确保只有设备所有者可以利用其存储的身份;
4) 在任何时候，用户的信息都将是明确的或公开的;
5) 由OriginalMy提供的解决方案是在登录时立即对用户提交的数据进行验证（复杂和自动化）的解决方案。
6) 此外，它也是市场上最完整的解决方案，因为它具有以下安全控制，全部不断升级：
    a) 生物测量;
    b) 用户和密码;
    c) 完整的属性注册;
    d) 自动验证注册数据，搜索公共网络中的信息，OCR和图像阅读;
    e) 仅在设备中存储区块链接ID;

而且，在合同签字的情况下，它将证明文件的所有权。

5.6合同签名 - 第2版（现在）

身份层结束后，我们开发了第二版平台签订合同。首先，它被用于比特币网络，并且在2017年5月交易的费用价值表现上升后，它被迁移到了以太坊平台，之后是以太坊经典。

合约签字平台于2017年5月在纽约共识会议上正式启动。在Apple Store和Google Play上，该应用程序允许巴西用户以直观的方式注册（即获取他们的区块链ID）并签署他们是签名者的文档，而与初始模型（视频证明）相比，摩擦更小）。

此外，签署的数字文件也已注册，双方可以通过OriginalMy平台验证其真实性。

5.7 侧链

目前的区块链在规模上有挑战，当涉及到他们可以做的注册处理的税收（tx / s）以及交易成本（费用）时。

比特币的设计可以承受7 tx / s，但实际上只有3 tx / s，而以太坊理论上设计使每秒数十万次的事务[19]达到15 tx / s的限制。

此外，信息熵最大的块状结构成本更高，注册信息的成本更高，按交易金额和成本限制了利润的大小。

由于这些原因，我们开始使用Decred [20]的DCRTime项目的定制版本进行文件的真实性注册，该文件基于在数字文档的时间戳过程中提供规模的模式[21] 。

随着这一功能的实现，在处理交易方面取得了显着的进步，开创了每秒管理数百万次交易的可能性，而不会显着降低性能或增加成本。

我们打算研究这种格式的签名合同文件的演变，允许更大的利润，无论是在加工量和降低成本。

将来，一旦完成了对合同签名的预测实施，侧链将作为开源（开源）

5.8 多个区块链

在2015年推出时，OriginalMy仅在Bitcoin的网络连接网络上注册了文件的真实性。

随着使用块链的协议的演变，并且鉴于我们对使用块链不可知的事实，今天，OriginalMy平台在4个公共块链以及其他私有块中进行注册，这是最相关的：

- 比特币: www.bitcoin.org

- 以太坊: www.ethereum.org
- 以太坊经典: www.ethereumclassic.org
- Decred数字货币: www.decred.org

这样，平台的设计非常灵活，根据与API环境集成的客户需求，进行注册。

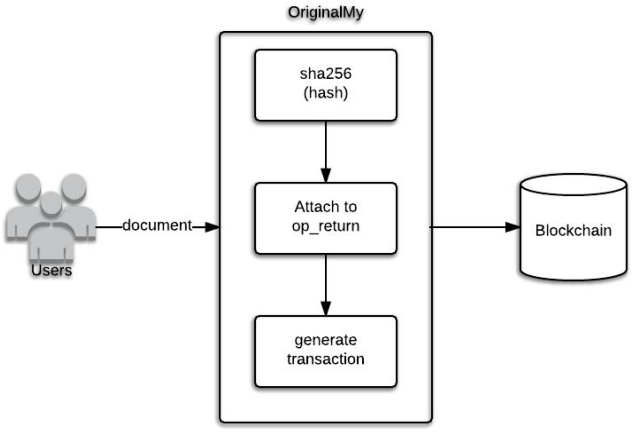
重要的是说，OriginalMy平台的设计和开发方式允许集成商开发其产品或集成，而无需了解现有块链的细节。处理这些应用程序的封锁层的复杂性是OriginalMy的全部责任，它允许可扩展性在可用应用程序的使用中，而不需要开发人员具有密码协议的具体知识。

6. 应用规格

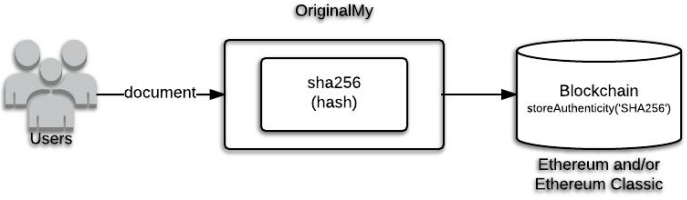
6.1 数字文件的真实性证明

最初，真实性的注册仅在文档的数字签名（SHA256 [22]）的注册表中存储，并存储在该网络的事务的op_return [23]的字段中。在包含其他块链之后，格式根据所使用的协议进行多样化。

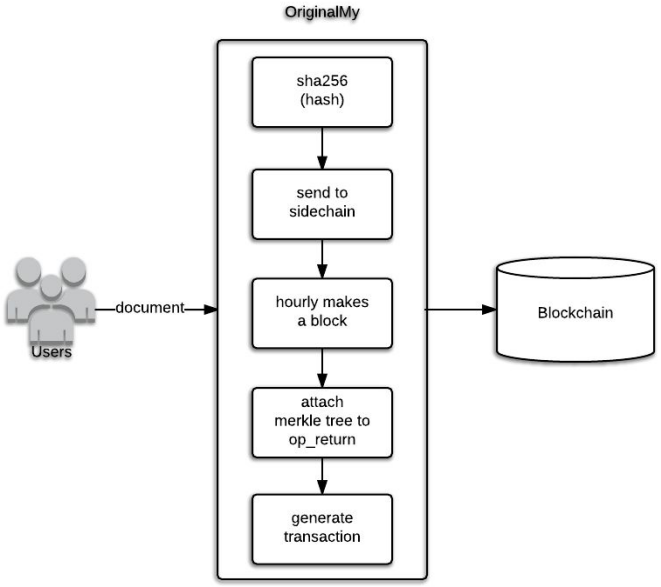
- 比特币：（sha256 +巴西法定时间+ OM标记）在字段op_return



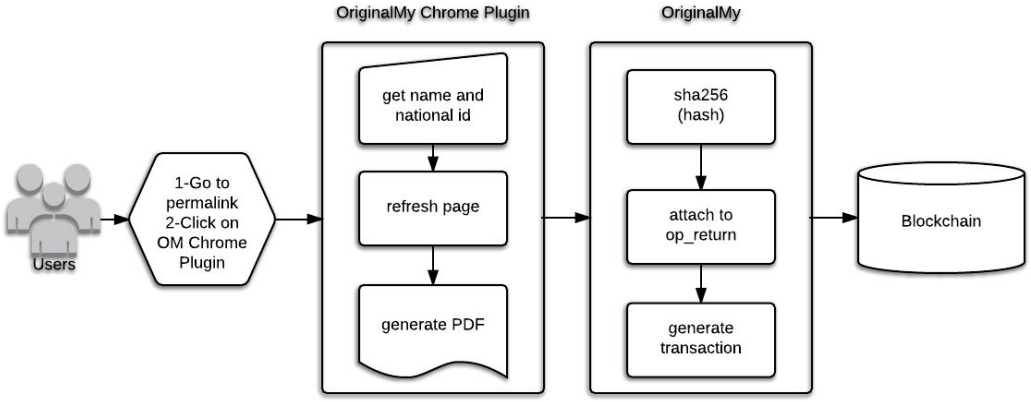
- 以太坊: https://github.com/OriginalMy/originalmy-dapp-addresses
  - Mainnet Ethereum >> 文件真实性
- 以太坊经典: https://github.com/OriginalMy/originalmy-dapp-addresses
  - Mainnet Ethereum Classic >> 文件真实性



- 在字段op_return中Decred：（merkle tree + OM marker）



6.2 网页内容的真实性证明



数字文件的真实性证明在每个区块链上的注册过程相同。

6.3 区块链ID

用户在应用程序注册的那一刻，它可以通过各种自动验证或自动化过程。这发生在三个步骤：

6.3.1 注册应用程序和初步验证

1. 创建用户和密码;
2. 电子邮件验证;
3. 电话号码和设备号码验证;
4. 公共数据库中的RPP验证;

5. 自拍照片的用户面孔，直接在应用程序上;
6. 文档图片，以可以将用户识别为文档编号的方式;和
7. 创建区块链ID，私人方只能存储在用户的设备中，而不与我们的系统或其他人员联系。公共信息发送到我们的服务器进行验证。

我们的系统，员工和协作者没有（也不会有）与用于生成区块链ID的单词联系，而是创建它的用户的属性的唯一信息。

区块链 ID与块中公开的用户的RPP号相关联，允许每天24小时，每周7天进行验证，允许该用户创建其01。

6.3.2 在公共网络上自动搜索

在创建帐户和区块链ID后，系统会在公共政府基础上进行搜索，以验证RPP，并将提供的数据与可公开验证的数据进行比较。

6.3.3 自动验证文件

在RPP验证，公共网络中的其他数据和信息后，系统将自动发送需要手动验证的信息给OriginalMy的验证小组。如果检测到一些不一致，则注册被阻止。用户只能在提供有效信息后才能使用它们的区块链ID。

6.3.4 授予区块链ID

基于使用块链的技术，使用非对称密钥加密创建块链ID。

区块链标识被公开存储在块链中:

- 以太坊经典: https://github.com/OriginalMy/originalmy-dapp-addresses
    - Mainnet Ethereum Classic >> CPF ID和钱包库

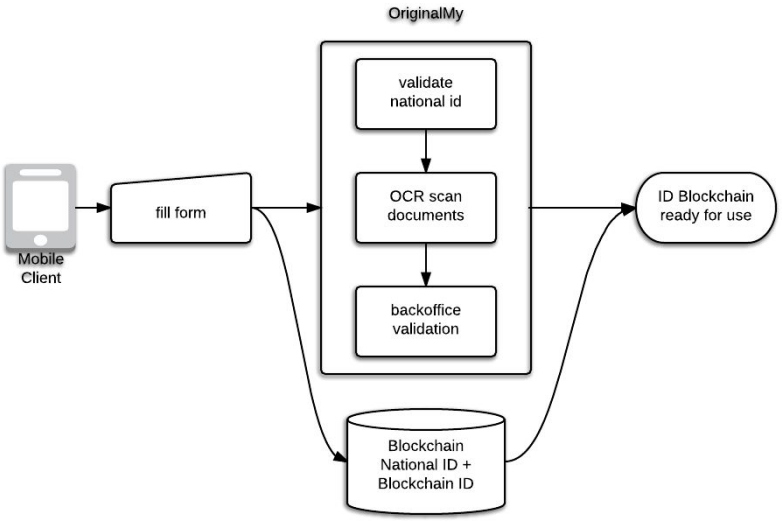
6.3.5 恢复区块链ID

在更换电话，重新安装应用程序或登录新设备的情况下，系统将再次要求验证数据。然而，在此之前，它将提供恢复以前提供的区块链ID的机会。

为此，将要求一组12个字，一旦提供正确将使系统恢复块链ID。

然而，如果用户在几次失败的尝试中没有字词或填写错误，则系统将自动进行创建新的区块链ID的过程，就像初始注册过程一样。

新的区块链ID将替换旧的区块链ID，并将在该设备中以公开的方式与该用户保持连接。因此，签署的合同和注册文件的所有历史将是完整的。



6.4 签发文件和合同

如上所述，最初的合同是在比特币网络的块中签署的，由于成本和性能的原因，协议被转移到了以太坊经典。

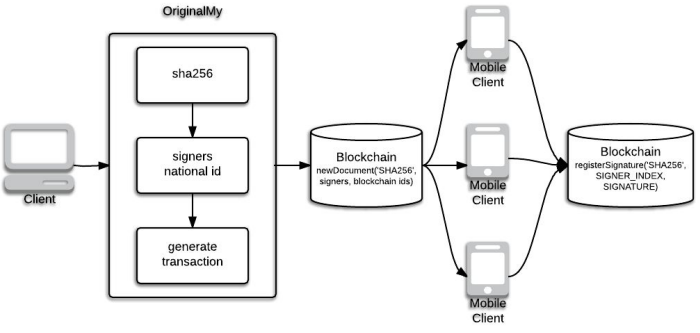
在这个意义上，尽管经济便宜，但是以太坊经典网络的交易速度更快：比特币网络的时间大约为10分钟，这样一来，文档的注册就会出现在用户签名的应用中，同样的时间通过使用以太坊经典减少到15秒。

6.4.1以太坊经典块状链的使用

如今的文件和合同是使用以太坊经典作为基础设施签署的。

在我们的系统中验证其身份后，用户可以使用它来执行数字环境的操作，从简单的记录中进行，而无需填写表单和注册（注册）和网站登录（登录），以庆祝复杂的司法业务合法接受，具有约束力和可执行性。

文件的签名是通过移动应用程序OriginalMy（安卓和苹果）进行的，证明了作者身份，并在签名时提供文档的所有权证明。



所有签名者签署文档后，智能合同会将*checkCompleted*标志提醒为*True*。正在监控签名过程的任何其他智能合同第三方可以自动继续此过程。

6.4.2使用比特币区块链

尽管目前由于成本而没有被使用，但是该协议先前被开发用于其他块链的迁移，并且可能最终被恢复。

如果是这样，它将以这种方式工作：
注册:

1. 在OriginalMy网站，提供合同的原始文件，并列出签名者的RPP
2. 使用信息创建1个交易：
    a. 系统生成一个钱包地址来识别合同（合同地址）
    b. 在op_return注册：[sha256 +合约的钱包+ OM标记]
    c. 在智能合同中搜索ID（IdRepo），列出所列RPP的区块链身份
    d. 电子钱包地址是使用带有hash160的RPP生成的：[sig; RPP]在hash160法律巴西时间生成的电子钱包地址：[t; timestamp]
    e. 即发送灰尘注册RPP和法定时间

验证：
验证合同的地址，并查找与用户的区块链ID的交互。

只有当用户使用移动应用程序签署文档时，才会发生此交互，从而在签名时证明文档的作者身份和所有权证明。
合同注册交易示例：
https://blockchain.info/pt/tx/523e63ad8a1cd928e7a5292f7145af3596bb11475750b466319e74d77003ef24

说明:
tx: 523e63ad8a1cd928e7a5292f7145af3596bb11475750b466319e74d77003ef24

- 1HyuB5rM3ZpP1cHqTCJLGs65usNkzDZiUU: 区块链ID 1号
- 1BXEycBEfCqYgPGebhkLBwKrp4VpbiHszV: 国际ID 1号(hash160十六进制编码)
- 1KaRgqmRSLwYFfeyHgpQaSnLsK3bVwpUqc: 区块链ID 2号
- 1BXEycBDsSGSGmWqgd6KrQN4Hu8RKTDCCa: 区块链ID 2号(hash160十六进制编码)
- 1BbaJGRHWCfX18bFKqyTSHGEm8QS7MBXAx: 法定小时(hash160十六进制编码)

op_return

- sha256: 971bbbc7e67522ec7df3fd523bf9d83899f376d0b3c66d5a2776420b178a84743
- 合约钱包: 15poB7iiLShugHLFpbfX5v3Nc4TkDbGJVR
- OM标记: ORIGMY

本合同签字交易示例：
https://blockchain.info/address/15poB7iiLShugHLFpbfX5v3Nc4TkDbGJVR

- 合约钱包: 15poB7iiLShugHLFpbfX5v3Nc4TkDbGJVR

验证*1HyuB5rM3ZpP1cHqTCJLGs65usNkzDZiUU和 1KaRgqmRSLwYFfeyHgpQaSnLsK3bVwpUqc*与本合同交互。这意味着双方都签署了文件。

7. 新平台

目前的*众售*目标是促进OriginalMy平台发展的新阶段。这个新平台将为数字环境下的身份注册，文档和签名提供全球解决方案，并启动Blockchain ID的完全分散化过程。.

一旦第01阶段的采用取得成功（检查项目8），将设计并开始开发一种以分散方式注册真实性的新特定块链，以数字标识为基础，如OriginalMy已经开发的一些应用程序。

重要的是要记住，尽管技术发展面临挑战，真品证明的权力下放过程涉及处理集中化信息的唯一目的所存在的传统公共和私人机构。因此，我们选择了正在建立网络和逐步分散化的过程，作为ABC代币的提供，同样分为两个步骤。

7.1 国际化

关于提供代币的第一个目标是OriginalMy平台的国际化的开始。为了做到这一点，将推动实质性的改变，这将允许其他国家的用户在区块链ID中注册，并根据预期的路线图。

7.2 用户体验

我们知道，块链中的解决方案需要解决实际问题，而不会引起摩擦，或导致交易和/或转换的巨大成本。因此，主要目标之一将是在Web环境和移动应用程序上已经可用的应用程序的导航性方面提供实质性的改进。

7.3 ABC 代币

随着众售的成功，OriginalMy平台媒体的所有可用功能将只能通过ABC代币访问（请参阅路线图进行实施）。在这个意义上，ABC代币将授予在OriginalMy平台上使用所有可用的应用程序的权利，并且可以是通过人群（通过二级市场）或直接从OriginalMy获得的网络推广特定程序的一部分，通过要实施的阳台（OTC，OriginalMy）。

7.4 OTC市场的 OriginalMy

为了使普及的OriginalMy平台成为可能，更不用说要创建的网络改进政策，我们还将创建一个我们自己的阳台市场，我们将直接向希望使用我们服务的用户销售代币。使用价格，未来参考价格目前固定为5.20新加坡元，将根据使用量和使用的服务种类以及使用的块状而有所不同。

一旦OTC可用，OriginalMy承诺，路线图一直在视线中，以最低的二级市场价格实行最低卖价。最初，我们估计，在二级市场上，OTC上销售的代币价格将至少比20年（二十%）在过去30（30）天内谈判达成的交易量的平均价值高出20%记录了ABC代币的谈判量较高：

场内购买

$$OTC\ Sale$$

$$min.\ Price = 1,2 \times \frac{\sum_{i=1}^{n}(pi \times xi)}{\sum_{i=1}^{n} pi}$$

即：
p =过去30天流动性较高的二级市场上ABC代币的协商量;和
x =过去30天流动性较高的二级市场上ABC代币的谈判价格

此外，根据机会和便利标准，OriginlMy可以在OTC 市场OriginalMy提供ABC代币的回购计划，可以根据其独家标准由ABC代币的所有者使用。在这种情况下，OriginalMy承诺实行的价格低于二级市场的平均价格。最初，我们估计，在二级市场上，OTC上销售的代币价格将至少超过80%（二十%），超过了在过去30（30）天内已经谈判达成的交易量的平均值。记录了ABC代币的谈判量较高：

场外购买

$$OTC\ Purchase$$

$$max.\ Price = 0,8 \times \frac{\sum_{i=1}^{n}(pi \times xi)}{\sum_{i=1}^{n} pi}$$

即：
p =过去30天流动性较高的二级市场上ABC代币的协商量;和
x =过去30天流动性较高的二级市场上ABC代币的谈判价格

我们保留在适当的时候更改现在预测的规则的权利，以便在被证明对我们的业务的发展和功能有好处的情况下。在这种情况下，我们将寻求平衡最终的改变与ABC代币持有者的利益，我们将通过OriginalMy的官方沟通渠道广泛发布。

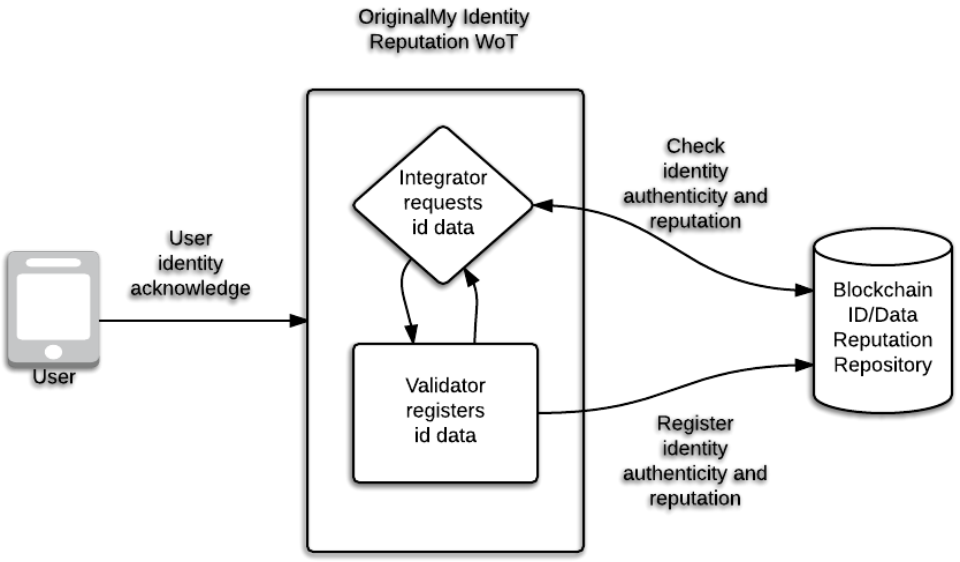
7.5 区块链ID的分散化

区块链 ID的解决方案可以通过应用程序（由OriginalMy或第三方开发）为多个行业的公司和社会带来无法估量的收益。为了真正实现这一点，主要措施之一就是分散集体的身份和属性的创建和验证过程，从而增强网络效应，创造出巨大的网络效应，并采用这个新平台。

使用与区块链分散促进的分散真实性相关联的Web信任资源，可以评估组成用户身份的每个属性的一致性和声誉。

在这个意义上，OriginalMy将负责提供这个新协议的架构和设计，并考虑到区块链 ID的安全分散化过程的一步一步，通过具体的激励来创建和推广新的分散网络刺激用户身份和属性注册

的系统，以及为节点（“证明证明”）确定和重新验证每个这些数据的奖励。



8.众售: ABC 代币

销售代币的过程分为两个阶段，因为它是巴西第一个提供代币功能的公司，也是世界上第一个在世界上第一个提供了已经发展和运行的技术平台的整个经济体系。

因此，我们始终对参与此过程的人谨慎和尊重，我们选择将代币销售分为两个不同阶段，作为已经描述的逐步分散化过程和有机创建分散式网络的目标。

8.1 阶段01

销售ABC代币的第01期目标是在平台的国际化进程开始之前提高资源，对某些国家公共基础的身份进行研究和验证，并显着改善用户体验（项目6.1和6.2）。因此，最低总额必须达到1,000,000.00美元的价值，这是为了执行这些步骤而估计的。

此外，通过额外的可用资源，可以将平台扩展到更多的国家，完成OriginalMy可用产品的完整“标记化”，并实施我们自己的OTC（项目6.3和6.4），使其成为经济将在市场上完全由可用的代币完全平衡的第一个环境之一。为实现这一目标，最低缴款总额必须达到3,000,000.00美元。

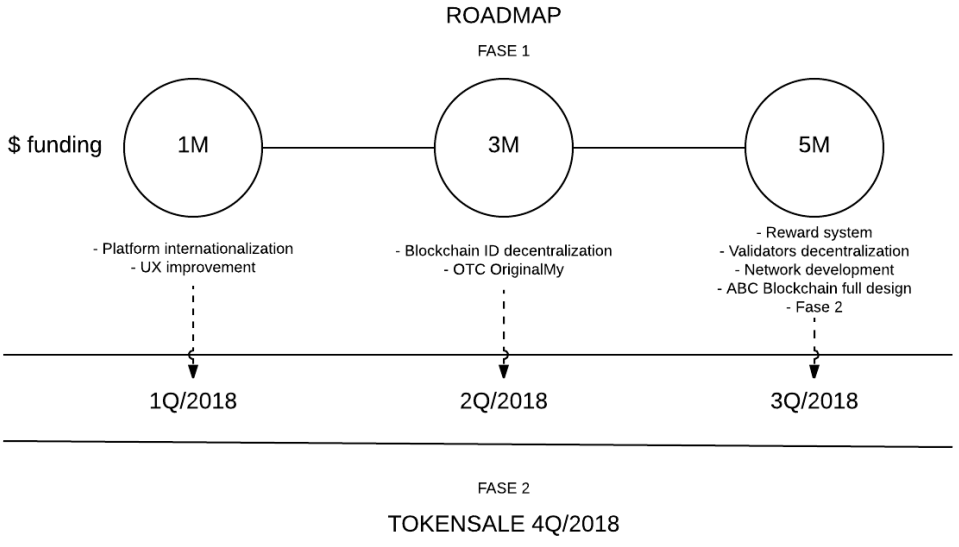
最后，如果报价达到了上限（5,000,000.00美元）的价值，就可以对数据验证者进行分散化，为验证者和用户创建一个奖励制度，促进一个全球性网络，还有一个原型架构并设计一个特定于真实性登记的新块（项目6.5），在第二阶段阶段加速新协议的创建过程，现在将对此进行描述。

8.2 阶段02

销售ABC代币的第02期预计将在第01阶段预测的路线图结束之后发生，并将为完成开发新的人员和组织身份和属性新协议的资源筹集资源， 将补充新的特定块链和自己的采矿规则。

致力于身份认证注册和验证，合同签字（法定业务庆典），资料和确定的资产转移的核心链条将促进注册的规模和低成本，限制当前封锁的项目。

报价条件将以机会性出现; 在这个阶段提供的ABC代币将已经发布，并且将在机会到来时保留供谈判。



8.3 新的区块链和代币交换

一旦代币销售阶段的成功完成，将开始开发一种用于分散处理真实性的新的开放源代码协议，该协议将以特定的封锁方式计算，这是一个非常自己的采矿和激励系统（如第7.5项）

在这种情况下，OriginalMy将建立一个代替用于访问OriginalMy平台的代币的程序，以及一个合理的时间表，并广泛地发布了已经发布了新协议的代币的ABC代币的交易，比率为1：1。

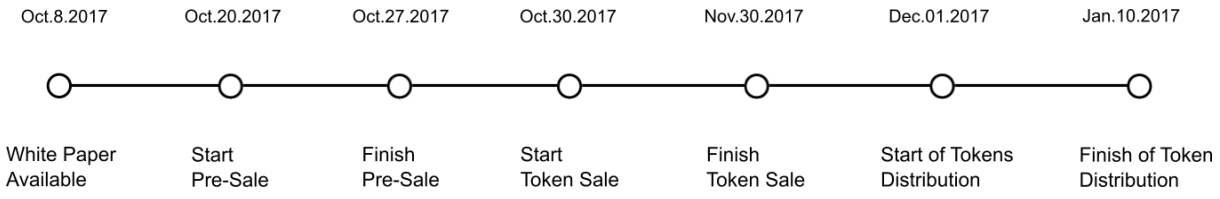
使用新的代币块链替代以太坊平台上发出的代币将使用Atomic Swap [24]或类似技术进行。

8.4 销售代币的时间表

销售第01阶段的代币（代币销售）将按照预先确定的关键日期（关键日期）的时间表，以指导整个过程。

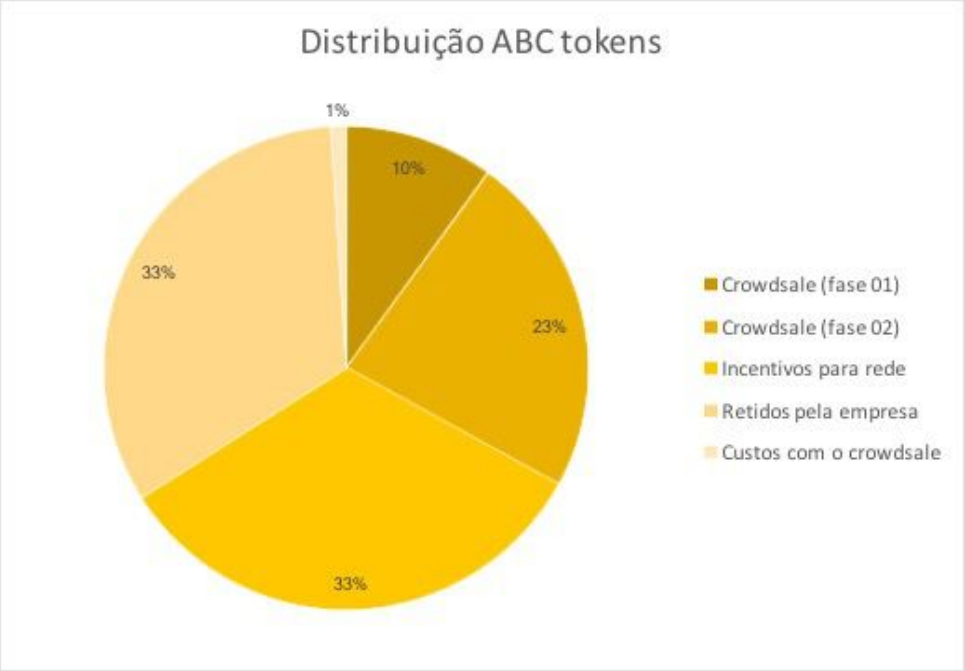
当所有在01阶段提供的代币被出售或达到代币销售的限制日期（以较先者为准）时，关闭将会发生。

代币销售阶段01的关键日期如下



8.5 代币的问题和限制期限

- 代币总数：将发行2亿（2亿）个代币，将按以下方式分配:
    - 33% 可用于代币销售（01期：10%，02：23%）；
    - 33% 将继续占有公司;
    - 33% 用于网络建设;
    - 1% 将用作众售费用.



- 团队授权（带或不带归属）：01阶段没有，但可以对阶段2进行审查。
- ICO推出：2017年10月07日推出专刊网站，白皮书和项目进一步文件将在此发布。那些希望参加人群的人可以从这个日期起登记他们的数据，并表明他们参与代币销售的意图。
- 预售：代币预售将于2017年10月20日至27日进行预售。在此期间收购代币将允许买方获得更多的代币，相对于开放后允许的最大金额的代币销售。
- 代币销售：代币销售的期间将在2017年10月30日至2017年11月30日之间发生。
- 代币交付：在代币销售结束后最多约一个月内，向买家发放代币，预计将于12月1日开始，至2018年1月10日止。

8.6 ABC代币销售的规则和条件 – 01阶段

为了销售代币以有组织的方式发生，并提供机会尽可能地参与最多的有关方面，必须遵守一些规则，如下所述：

- 官方频道：代币销售将专门在网站https://originalmy.com/ico上进行，其中可以获取ABC代币，只要人气规则得到尊重。 OriginalMy将不对发生的任何报价，购买和/或销售或上述网站之外的任何谈判负责。

- ABC代币：代币将使用以太坊平台发行，格式为ERC20。要发行的代币总数为2亿。

- 提供的代币：在人群阶段提供的代币总数将相当于发行的ABC代币总额的33%，即从这20万美元中，10%对应于ABC代币的总额，将在此出售机会，每个代币的价值为0.25美元。

- 批次销售：可在01期出售的代币将分开批出，销售开放时公布。

- 参与限制：只允许参与者获得01（1）个代币。因此，一旦完成购买，就不可能再次获得代币或任何已经完成的收购数据。

- 付款方式：可以使用比特币（BTC）或以太网（ETH）对ABC代币付款，不接受其他付款方式。

- 付款地址：Bitcoin和Ethereum数码钱包的地址只会在付款时给予买家，完全由人群发生的网站。 OriginalMy不会以其他方式提供用于支付代币销售的钱包的数字地址，也不会以其名义授权其他人。因此，对于与人群官方网站上提供的钱包不同的钱包地址的任何付款，不承担任何责任。

- 付款确认：ABC代币的付款仅在比特币网络进行至少6次确认或由Ethereum网络进行的30次确认后才会被确认。一旦交易确认，OriginalMy将通过电子邮件通知，通知参与人群的成功。

- 支付价值中的差额：以不同价值收到的收取所需ABC代币费用的付款将被参与者退回到通知地址，即取消购买请求。

- 付款时间：一旦ABC代币的采购订单进行，付款必须在购买时最多30分钟到达发布的地址。如果在这段时间内没有付款，买方将取消其采购订单。

- 最低贡献价值：如果代币销售额不超过1,000,000.00美元，人群将被取消，所有购买都将退还;

- 退款：如果任何导致买方存放的价值的事件按照上述条款退还，则矿工处理此类退款所征收的税款将从原始存款值中扣除，在这种情况下，返还净值。

8.7 法定处分

a) OriginalMy应用程序的法律全景

OriginalMy平台提供的应用程序是根据适用于细节的合法性原则开发的，并以巴西立法为基础（特别是公共法律法律[法律6,015 / 73]，数字程序法[Lei 11.419 / 06]和关于数字环境签字的剩余立法[临时措施2200-2 / 01和法律12.682 / 12]，反洗钱政策和COAF，BACE和CVM的KYC）和外国（特别是涉及到UE 2015的指令/ 849，金融行动特别工作组（FATF）和稀疏KYC / AML / CTF规定）。

b) ABC代币的法律全景

根据要机会发布的条款和条件，ABC代币代表在OriginalMy平台上机会地提供产品和/或应用程序的使用许可。

这样，上述标记根据定义和最终确定，没有具有利润预期的代表金融投资的范围。因此，他们没有证券的性质，他们不会通过分配任何价值和/或分享或授予其在政治和/或经济，现在或未来的权利，通过OriginalMy授予其所有者的利润期望。

9. 团队

OriginalMy团队由实验人员组成，并在相关专业领域取得相关成就。

Edilson Osório Junior - 创始人兼首席执行官

计算机科学家，数据处理技术人员，信息安全和基础设施方面的老师和专家，拥有25年市场经验。毕业于哈佛法学院版权所有。他在巴西和拉丁美洲的区块链参考，毕业了数百名开发人员，并介绍了巴西市场的主题，被邀请参加公开和私人活动（包括国际活动）的讲座，讨论区块链以及由OriginalMy造成的干扰。
https://www.linkedin.com/in/osoriojr

Miriam Tomie Oshiro - 联合创始人兼首席财务官

化学家和化学工程师加工工程专家，2002年起她在USP的化学工程系在环境科学研究领域开始工作，之后在塑料，贵金属和重型机械领域的大公司。她是Daruni Healthcare任职4年的运营总监
https://www.linkedin.com/in/miriam-tomie-oshiro-6a4b9223

Renato Martins da Silva – CTO市场

开发人员毕业于FIAP，自2001年起就在发展领域工作。
代表GED的伟大国家公司和政府有关数据处理和文件分类的政府项目。
https://www.linkedin.com/in/renatomartinsdev

Helena Suarez Margarido - 法律与合规

律师毕业于PUC-SP，在美国（伊利诺伊大学）和欧洲（葡萄牙天主教大学）学习法学硕士学位。 Blockchain和数字硬币专家5年，在巴西和国外的教师和讲师，拥有15年的经验（GP，投

资，普华永道，Itaú银行）。 Suo Law办公室的创始人合伙人，InversaPublicações的作家和比特币研究所的联合创始人。
https://www.linkedin.com/in/helenamargarido

Rafael Matos Araújo - 开发者

机械工程师毕业于临PUC米纳斯。在工业工程师部门工作了5年，对大型巴西公司如淡水河谷（Vale）和巴西石油公司（Petrobrás）进行了大量工程;
https://www.linkedin.com/in/rafamatosaraujo

Renato Novaes de Abreu Neto - 开发商

自学和科技爱好者。选择Web编程作为主要焦点。 Chatbots和Web爬虫处理经验。
https://www.linkedin.com/mynetwork

Fernando Henrique Corrêa - Developer

在2004年开始使用免费软件开发职业生涯。在开发用于酒吧，餐厅的软件的开发中，这是该细分市场的参考。以Mandic先生为首，在巴西提供互联网。是UOL开发团队的成员，巴西最大的新闻门户网站，使用DevOps作为开发环境基础设施的重点
https://www.linkedin.com/in/fernando-henrique-corrêa-98b55920

10. 参考文献和参考书目

10.1参考文献

[1] 2017 Index of Economic Freedom: http://www.heritage.org/index/country/brazil (Oct/2017)
[2] Federa Public Ministery: http://www.mpf.mp.br/para-o-cidadao/caso-lava-jato/atuacao-na-1a-instancia/parana/resultado (10/04/2017)
[3] G1: http://g1.globo.com/pr/parana/noticia/2015/11/pf-estima-que-prejuizo-da-petrobras-com-corrupcao-pode-ser-de-r-42-bi.html (10/04/2017)
[4] Central Bank of Brazil: http://www4.bcb.gov.br/pec/taxas/port/ptaxnpesq.asp?id=txcotacao (10/04/2017)
[5] RIBEIRO, Mario Sergio - Pós Graduação Lato-Sensu em Gestão de Segurança da Informação no Instituto de Pesquisas Elétricas e Nucleares da USP (IPEN) - 2003
[6] Orange Book, cap. 5 e 6. - Padrões de Segurança do Departamento da Defesa dos EUA: Critérios para a avaliação de sistemas computacionais confiáveis.
[7] WEBER, Max. “O que é a Burocracia?”, ed. Conselho Federal de Administração, p. 37
[8] OLIVEIRA, Gercina Alves de; “A Burocracia Weberiana e a Administração Federal Brasileira”, 1970, R.A.P, Rio de Janeiro, p. 54
[9] YouTube: https://www.youtube.com/watch?v=gHK9HhzaPog
[10] Bitcoin: A Peer-to-Peer Electronic Cash System. Nakamoto, Satoshi, cap 6: Incentives https://bitcoin.org/bitcoin.pdf (10/02/2017)

[11] Ethereum Homestead:
http://ethdocs.org/en/latest/contracts-and-transactions/developer-tools.html (21/07/2017)
[12] Characterized by the borrowing of Information or any data for the utilization by a third party, generally a person with a bond or trust. Eg: credit card of a dad by his son, without the authorization of the first.
[13] Chamber of Deputies: http://www2.camara.leg.br/participacao/sugira-um-projeto (10/04/2017)
[14] Google Impact Challenge | Brazil:
https://desafiosocial.withgoogle.com/brazil2016/charity/its-rio
[15] Mudamos: http://mudamos.org
[16] Hashcash: http://www.hashcash.org
[17] Github: https://github.com/OriginalMy/OrigMyID
[18] Github: https://github.com/bitid/bitid
[19] Ethereum Blog: https://blog.ethereum.org/2014/10/21/scalability-part-2-hypercubes/
[20] Github: https://github.com/decred/dcrtime
[21] Open Timestamps: https://opentimestamps.org
[22] Wikipedia: https://en.wikipedia.org/wiki/SHA-2 (07/21/2017)
[23] Bitcoinwiki: https://en.bitcoin.it/wiki/OP_RETURN (07/21/2017)
[24] Github: https://github.com/decred/atomicswap

10.2参考书目

[A] Anti-Sybil Mechanism against Bogus Identities in Social Networks:
http://ijartet.com/papers/issue2/V01I020925.pdf (10/04/2017)

[B] Verifying Program Executions Succinctly and in Zero Knowledge:
https://eprint.iacr.org/2013/507.pdf (06/10/2017)

[C] Enigma: Decentralized Computation Platform with Guaranteed Privacy
https://www.enigma.co/enigma_full.pdf (06/10/2017)

[D] Hawk: The Blockchain Model of Cryptography and Privacy-Preserving ...
https://eprint.iacr.org/2015/675.pdf (06/10/2017)

[E] Pseudonym Parties:
An Offline Foundation for Online Accountability:
http://www.brynosaurus.com/log/2007/0327-PseudonymParties.pdf (06/10/2017)