白皮书 | 以太坊上的去中心化自治组织管理应用：Aragon白皮书

Aragon Network: 去中心化的价值交换基础设施
版本1.1（2017-04-20）
作者：Luis Cuende（luis@aragon.one ）
Jorge Izquierdo（ jorge@aragon.one）

摘要

Aragon Network（阿拉贡）是一个由代币控制的数字管理组织，专注于为经济增长创造最好的条件。本质上，Aragon Network是个可以让任意组织、企业家和投资人高效安全协作，并且没有技术漏洞和恶意参与方的生态系统。

Aragon Network的链上组织将会使用Aragon Core进行搭建，它是由一个Solidity语言的去中心化自治组织（DAO）和网页端去中心化应用（dApp）组成。一开始，Aragon Core会专注于资本化的公司类组织，但它的模块化功能也足够适应其他种类的组织。

这篇论文首先讨论了一个链上组织的原则和Aragon Core的功能，之后讨论了Aragon Network的代币模型和网络治理模型，最后定义了Network的成功所必须要保证的两个服务：去中心化的法庭 和 升级机制。去中心化的法庭 将会为无法写进智能合约的人际冲突提供仲裁服务。Aragon Core组织的 升级机制 能够适应主流非技术用户的需求。

Aragon Project建立在过去数十年间、数千人的努力基础上。然而，我们希望特别指出几个极大地影响了Aragon的人们：
1、Ralph Merkle，是公钥密码学、Merkle树[1]的发明人之一，还有很多其他包括DAO民主等方面的广泛研究，很大地影响了Aragon的思想。
2、Satoshi Nakamoto，比特币的创造者[2]。
3、Vitalik Buterin，以太坊的创造者[3]，DAO概念的发明者，诸多文章的作者。
4、整个以太坊社区的开发者，为了他们关于Web3.0的工作和使dApps成为现实。

现在的论文早期给一些以太坊社区和区块链社区的个人看过，作者们非常感谢他们为了Aragon Network更好的设计而提出的评论和批评，当然另外剩下的一些错误还是作者的。

1. 介绍

1.1. 关于Aragon Core

Aragon是以太坊区块链上的一个可以让任何人创建和管理任意组织（公司、开源项目、非政府组织NGO、基金会、对冲基金…）的dApp。

Aragon实现了股东名册、代币转账、投票、职位任命、融资、会计等组织机构的基础功能。Aragon链上组织的行为可以轻易地通过修改章程来自定义。另外，Aragon组织还可以通过连接智能合约的第三方模块进行扩展。

1.2. 现有限制

以太坊区块链的诸多特性提供了创造和管理去中心化组织的独有机会，包括记录的不可篡改、透明性和快速交易。但是为了满足人们交易和价值创造的多个需求，还是需要在其之上新加一层，来实现所有这个系统参与者的激励问题。

在设计Aragon Core时，许多不利于人们使用去中心化方式进行创建、管理和协作的问题被解决掉了，包括：

- **主观余地**：智能合约可以编码大部分可能的合约接口，但人际关系中总有主观的成分，一个完全公正的系统需要考虑不能完全在智能合约里解决的冲突情况。
- **软件漏洞**：软件错误不可避免。软件可能会包含漏洞，所以软件需要很能够容易地升级，而且需要存在一个合理的漏洞报告悬赏机制，用于激励潜在的攻击者来发现漏洞而不是直接攻击。
- **奖励系统**：目前阶段，一些特定的协议和系统的货币化还没有完全确定。一些参与者是促成组织机构的关键，所以需要一个简单的奖励机制。

2. Aragon Core组织

2.1 组织说明

一个组织有很多需求，主要的几个：

- **身份**：这个是首要支柱，因为我们需要在和别人交互前，知晓每个实体的身份。
- **所有权**：股权是一种对创始人、投资者、顾问、合作伙伴和员工的奖励，还可以决定公司的所有权和方向。
- **投票**：公司的股东应该能够对公司的决定发表意见，这里会和所有权相关联。
- **资本**：创业风险很大，需要很多资源来运营和成长，包括以投资或贷款为形式的资本。
- **人们**：组织最终还是由人组成，需要简单的拉拢他们（身份）和奖励他们（薪水）的方法。
- **外联**：一个公司需要瞄准他们的用户来让他们购买公司的商品。在互联网上，有一个域名就足够了。
- **支付处理**：组织需要获利。需要存在一个简单收款的方法。
- **会计**：为了管理费用支出、烧钱速度和商业决定，需要维护一个会计账目。
- **保险**：一个公司有很多风险，通常需要买保险来应对意外事件。

上面这些有些有依赖关系，最终形成了一个闭环：

- **身份**：没有依赖
- **所有权**：依赖身份，因为你需要确保自己合作的是正确的对象

- 投票：依赖所有权，因为所有权意味着控制权
- 资本：依赖投票，因为意味着发行股份
- 人们：依赖资本，因为你需要招聘人

2.2. 实现

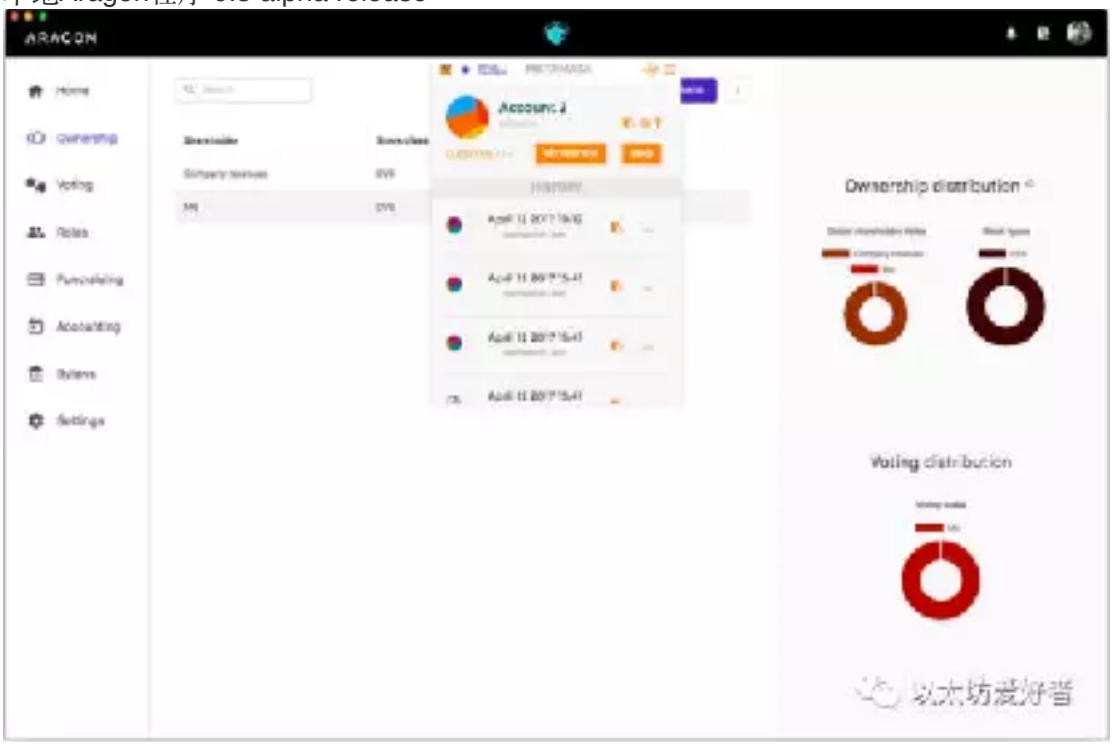
A． dApp环境

以太坊开发环境的一个好处是，有很多种方式可以运行dApps。我们在考虑Aragon的运行环境时，比较了各种选择的优缺点。

尽管Aragon Core可以作为一个纯净的dApp，运行在上面所有的环境中，我们最终还是用Electron实现了一个本地的程序，它安装简单，用户界面也熟悉，还把MetaMask加了进去。

我们将会推动这个本地程序作为默认的Aragon体验，我们觉得它对用户很友好，可以给从没听说过以太坊的人介绍，并让他在15分钟内发起一个Aragon Core组织。

本地Aragon程序 0.3 alpha release



B． 身份

我们已经开始集成Keybase，然后你就可以在区块链中设置身份信息了。[Aragon如何落实身份]。当发行新的代币给用户、或者用薪水招聘新的职员时，你需要确定你在给正确的人转账资产或钱。你可以每次都对收款人地址进行手工确认。Aragon会集成不同的身份提供商，现在我们在尝试uPort。我们在Aragon博客[4]里发布了一些关于dApps里身份的想法。

C. 权限

由身份引出了权限，我们预期了如下几种：

- 股东：有获取分红的权利，有转让不超过一定限额的股份给第三方的权利（这个比例通过投票决定的）。
- 执行人员：有更多的权限，可以做很多事务而不需要经过投票。

然而，去中心化无信任（或少信任）的组织可以允许和个体之间更宽松的关系。Aragon组织拥有自定义的章程允许定义谁可以执行哪一项业务（比如，经理可以给员工发薪水），或者业务开展的条件（比如，发行新股需要投票）。

D. 声誉

声誉在自由市场是非常有价值的，我们希望所有的业务合作都可以被评分。这允许组织可以评判一个承包商，同时承包商也可以评判一家公司。因为我们有所有关系的审计痕迹，可以轻易地追溯真实的交易。如果需要，这里可以完全匿名。

E. 初始化

当打开我们dApp后，你首先要创建一个以太坊账户，并安全地备份它，之后你可以选择：

- 输入你想要操作的公司的合约地址。
- 部署一个新的公司合约，然后我们dApp会自动跳转到这个合约地址。 初始化的过程需要对任何人都很简单，不仅仅是对加密货币熟悉者。

F. 所有权

Aragon Core组织中的所有权是透明和可转让的。每个股东的持股是公开的，并且股东有权转让股份给第三方。Aragon Core中制定了四种功能：

- 股东名册（和他们的持股比例）
- 股份转让，任意或有限制地
- 卖出或代币转账
- 发行新代币

组织可以发行有锁定期或其他限制转让条件的代币，所有发行的代币都将遵守ERC20代币标准[5]。这意味着股东的地址可以和一个名字或标签联系起来，或者通过安全的身份生成器获得。

G. 资本

创业公司需要快速融资。对于传统创业公司，他们可以找VC、通过第三方众筹（Kickstarter）、申请商业贷款、或麻烦亲戚朋友。Aragon Core组织可以很方便地在交易所发行新股，而不需要依赖第三方，通过直接销售或公开发售的方式：

- Aragon Core组织可以直接发行股份给某参与方，只要他转了事先谈好金额的货币。
- 如果一个组织想在市场上公开融资，Aragon可以在市场上公布融资需求，投资人可以先联系后谈判，或直接按照最大上限进行投资。

H. 奖励

传统的雇佣和薪水支付有很多不必要的麻烦，Aragon Core简化了这些流程。公司可以在某些条件下用薪水或发行代币来招聘员工，依据时间或任务表现。

这样就会有比较简单的界面，你可以选择要支付的金额、频率、股份和条件。为了使这个过程更高效，奖励可以是以太坊上的任意代币（使用类似0x协议[6]的去中心化交易所）或任何通过Cosmos或Polkadot可以进行跨链交换的加密货币。

如果喜欢法币，还有一种选择是自动创建一个用公司资金授权的预充值的信用卡。像Shake这样的方案，有一个API来生成临时的匿名的VISA卡来直接与软件交互。公司可以给员工或承包商进行评分。

I. 支付

对于收款支付，客户可以买入加密货币，然后通过ShapeShift的服务转换成企业家的货币。当用户获得加密货币后，他们就可以继续支付了，但其实只需一步操作，所有事情都在后台处理。我们预见到这是初始阶段的常用流程，而不需用户立刻创建他们的钱包。我们会连接加密货币交易所或提供商，来简化用户体验，就像Stripe一样。

J. 会计

会计模块是完全集成进去的，我们会最终提供接口给第三方进行形象化的展示，免去重新开发。

2.3. 模块软件

Aragon Core是在以太坊上运行一个组织所需的最小实现（参见上一节关于原则的定义）。然而组织有不同的需求，可能Aragon Core里没有拿来就能用的。为了解决这个问题，我们把Aragon Core设计成了，支持在其基础上再开发额外的功能（2.5节有技术细节）。

我们还预见到开发者会在与组织创建或运营无关的场景里使用Aragon Core，潜在的用例有：

- 政治选举投票模块，只是一个小的预测市场，给投票正确的人以奖励。
- 供应商支付模块，为供应商的完工或阶段性成果进行支付。
- 会计模块，拥有丰富可视化数据展示功能的会计模块（超越**Aragon Core**可以提供的）

很重要的是，所有的模块都可以使用标准的网站开发技术完成。这使开发者可以使用他们喜欢的任意工具，同时保留强大的沙盒功能和安全性。

2.4. Aragon Core简介

Aragon Core里主要是自定义的组织行为模式。简单说，Aragon Core的应用层的主要部分有：

- 规章系统：谁可以执行某项操作。
- 治理系统：如何做决定。
- 资本系统：发行和管理代币。
- 会计系统：管理资金。

所有部分一起工作，最终用去中心化的方式达成高效和公平的组织。另外，系统模块化的本质使Aragon Core组织可以根据自身需求自定义软件，或改造Aragon Core去适应其他应

用（比如政治选举投票）。Aragon Core会实现一个模块系统，将来更多功能可能建立在其之上。

3. DAO架构：内核，组件和应用

接下来的几节讨论去中心化自治组织[7]（DAO）的最小化定义，被Aragon Core和Aragon Network采用的DAO的哪些原则，还有DAO内核的基本结构和功能。

3.1. DAO的最小化定义

我们认为DAO需要用它的最小含义来定义，那就是：一个组织能够自我更新[8]，且维持永久的身份。

3.2. DAO的原则

在定义DAO核心的不同组件之前，我们先定义我们要完成的DAO的几个基本原则：

- 她是。我们需要认识到DAO是作为一个永恒的实体存在于世界上的。
- 一个DAO会一直存在除非她决定终止，届时就会永远消失。
- 一个DAO可以自我更新大多数基本组件，而仍被视为同一个实体。
- 她有。一个DAO拥有内部资本，因此也就拥有财产，原则上都是数字资产的形式（加密货币、代币、或者例如域名IP等的数字资产）。
- 她做。她可以操作外部世界或自身。她的软件执行用智能合约编写的代码。
- 她治。在事先编写的行为之外，外部的人们或机器行为也可以引发特定的DAO操作。

3.3. 内核功能

内核的核心功能是注册器，安排其他组件的优先级。每一个优先级只能存在一个组件，所以如果在一个已有的优先级设置一个新组件，就会替换掉老组件。内核的责任是接收不同种类的交易，并且使用统一的API分发给其他的组件。目前内核支持的接入交易有：

- 标准转账，用以太币转账：通过附带了币的以太坊交易。
- 预授权转账，用以太币转账：内核支持特定发送者对DAO的已签名的预先调用。发送者可以预先签名一个特定交易内容，并提供签名(r,s,v,币值)给某个可以代表他们利益的参与方。这可能需要另一个合约或状态通道来实现。
- 代币转账，我们认为代币在价值存储方面的功能等同于以太币，并且我们相信在应用程序里代币和以太币一样强大。内核会为所有标准函数支持用代币进行转账（有数据和功能调用）。对于ERC23代币接收接口和ConsenSys的HumanStandardToken的approveAndCall工作流的实现也已经准备好了。

在前两种情况下，价值通过以太币传输，内核会把以太币代币化为标准代币。这样DAO就可以对任意代币化的资产实现一个统一逻辑，而不用再区分以太币和代币。

内核会首先询问优先级位于1的组件，询问将要执行的这个操作是否被该实体所允许。如果不被允许，这个交易会在这个时点失败并终止。如果允许，内核会跳转该交易给优先级为1的分发组件（第一个组件）。

3.4. 内核的基本组成

A. 分发组件 – 她做I

分发组件的逻辑是会询问层级结构的上层预言家，这个操作是否是被该实体允许的。内核将会在执行任何操作前都询问这个。分发组件会分发进入的任意交易给能够执行该交易的组件，如果没有组件能够执行就失败。她会先检查这个操作是否是给自己的，不是的话按照优先级询问每个组件她们能否处理这个操作，如果可以就分发给她。每个操作将只会被分发给第一个能执行它的组件。

B. 信息组件 – 她是

这个组件会负责DAO的自我更新和自我毁灭。她会负责更新DAO内核的根引用和其他组件的注册。

C. 保险箱组件 – 她有

这个组件负责保管DAO拥有的资金和资产（代币资产），还负责怎么花费它们。

D. 代币组件 – 她治

这个组件负责追踪所有的能够管理DAO的治理代币，还包括一些添加、替换、删除代币的逻辑。

E. 应用组件 – 她做II

DAO的应用层会是自身的组件，这个组件将只会与其他组件有很少的交互（沙盒）。应用层这里有该组织的大部分业务逻辑。还会安装不同的应用（以太坊智能合约的形式）来为DAO提供更多功能性。我们会创建一个模块或应用商店，组织可以简单地安装可复用的组件。

4. Aragon Network

Aragon Network（AN）会是第一个去中心化自治组织，其目标是充当数字司法权，使组织的企业家和投资人可以非常容易地操作。

Aragon Network会从一个经过投票而成的非常简单的宪法启动，新的法律会通过治理机制被添加进来。

Aragon Network很重要的角色是保证网络内组织的成员关系，并检查他们是否遵守了发布的规则。

网络会通过积累用户在组织内的交易手续费来运转，这些手续费会贡献为网络的内部资产，由治理组织随意支配。这些资金的主要流向是给网络的服务提供者，这对网络的运行很必要。这些服务主要有：

- 开发支持运行去中心化组织的**Aragon Core**合约
- 一个去中心化的法庭（附录**A**），可以用来冻结组织
- 一个为所有**Aragon Core**提供合约升级和漏洞悬赏的服务

我们可以说Aragon Network会提供能为组织带来繁荣的所有事情，如果要跟现实世界做个类比的话，最好的例子就是今天的特拉华州为公司、投资人和企业家所做的事情。Aragon Network会是更有效率的区块链上的数字特拉华州。

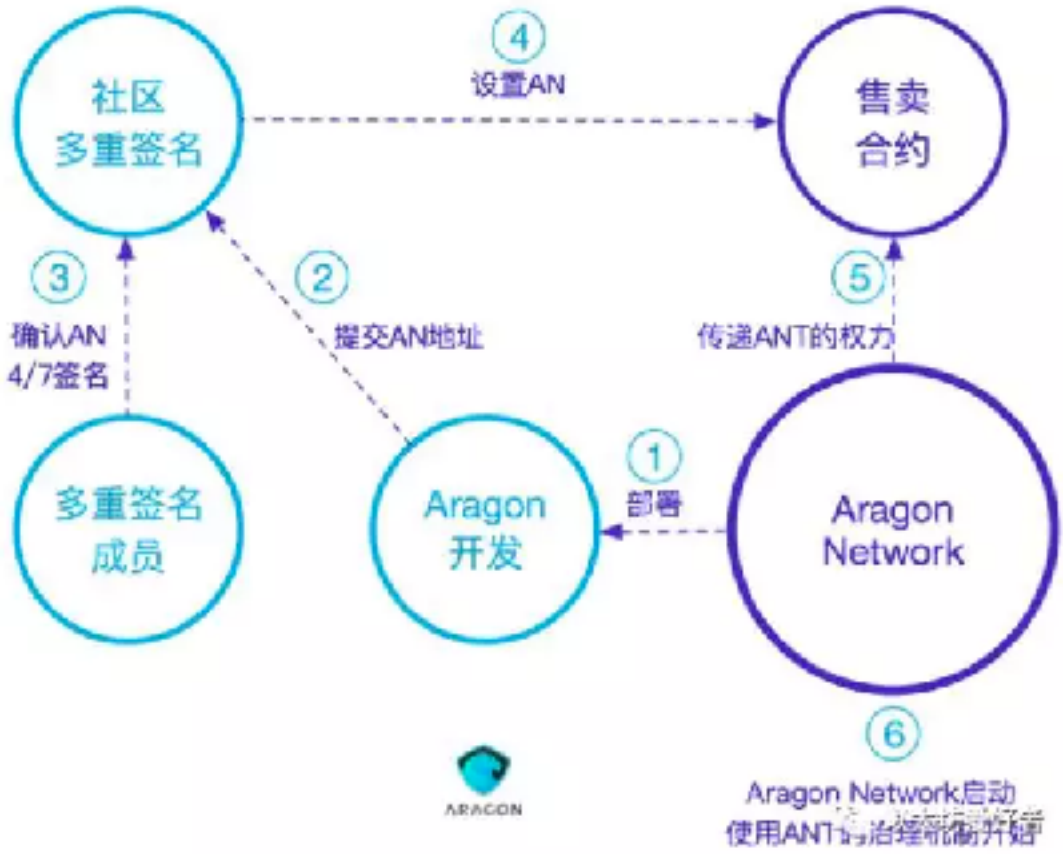
5. Aragon Network代币，ANT

跟货币代表了宏观经济的财富一样，ANT代表了去中心化经济体Aragon的财富。

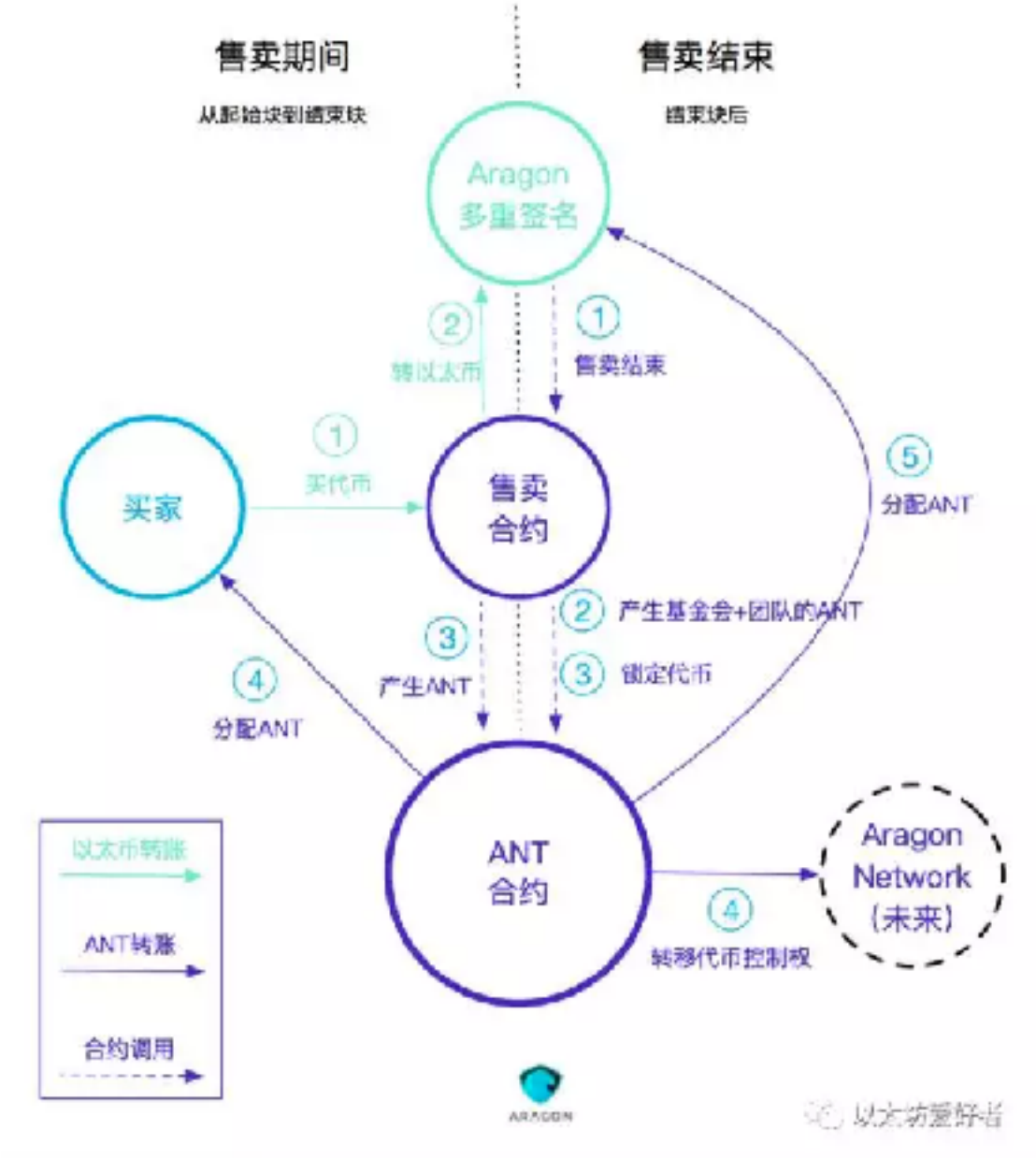
5.1. Network的启动和ANT发行

为了网络的启动，一个不限定上限数量的ANT会按照预先设定的随着时间而增长的价格进行售卖。ICO筹集的资金会交给Aragon基金会来资助Aragon Core和Aragon Network的开发（图5.1B）

售卖结束的某些时候，只要他们觉得实现了初始的目标，并且已经安全了，社区成员就会通过多重签名的方式部署Aragon Network。网络就在这个时刻启动，并且ANT持有者可以通过治理机制达成决议。



（图5.1A：Aragon Network部署机制）



（图5.1B：Aragon代币售卖机制）

5.2. 持续的代币模型

在初始售卖和网络部署后，ANT会持续增发。增发新的代币会有成本，作为加入网络而支付的一部分手续费会被用来资助发行新代币。这就有了向Aragon组织支付手续费的激励机制，组织贡献更多也就会收获更多ANT，也就意味着该组织在网络决策中会有更大的影响力。

增发新代币所需的费用由ANT代币持有者决定。这会是一个持续的决定，同时要考虑到经济学里的供需原则。如果增发新币成本过低，越来越多的代币就会进入流通，直到供应严重超出了需求。这个通胀的方案会让单个ANT代币的价格下降。最终，我们认为代币持有者将会决定出一个健康的均衡通胀率。通过同等对待每一个持有者的意见，市场会正确地反映最好的增发费用。

5.3. Network的治理机制

最开始，Aragon Network会是一种流动的民主[10]（换句话说，就像无政府状态[11]），来决定代币发行、资金分配、网络规则（看图5.3中关于ANT代币持有者能做的决定示例）。这意味着通过提案和投票系统，Network被部署在链上治理机制的基础上。这个机制决定了允许建立提案来升级这个机制本身。

ANT发行：

- 为ANT收入设置税收比例（可能低点，以鼓励使用ANT）
- 给全体代币持有者分配资金
- 从网络中关停或冻结不遵守规章的组织

资金分配：

- 将资金作为一次性奖励分配
- 为服务提供者重复性地分配资金
- 给全体代币持有者分配资金

网络规则：

- 建立宪法的规章
- 废除规章
- 从网络中关停或冻结不遵守规章的组织

5.4. Network的适应性

Aragon Network会提供一系列使去中心化组织广泛应用的基本服务，我们也希望她尽可能地保持全球化和开放。

Aragon Network有一些基本的宪法和治理方法，每个人都可以在Aragon里建立另一个只使用法律子集的网络。例如你可以创建一个组织，加入到Aragon Network，然后投票产生一个专门用于你自己组织的法律子集。或者该组织可以把Aragon Network的基本宪法服务作为一个框架，然后建立一个规则子集来治理组织间的关系。

5.5. 代币将来的应用

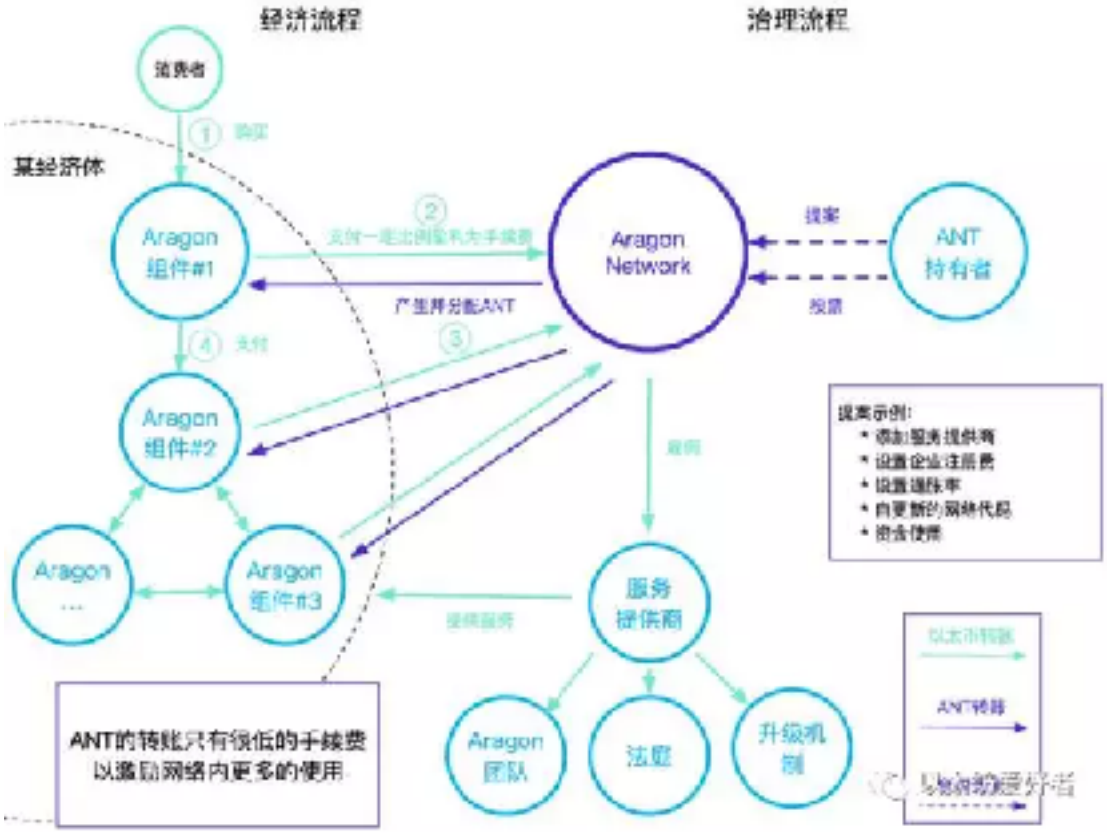
ANT会是所有网络服务的原生代币，不论是治理机制还是其他功能。比如在法庭功能中，持有者能够使用它们的代币来帮助裁决并获得奖励。

5.6. 代币技术特性

ANT会兼容ERC20标准，只是另外增加一些比如能否复制和锁定期等的特性。

6. 总结

AN通过提供能够在大范围内运行，且能够使组织高效运作的服务，解决了运行完全去中心化组织的核心问题。它提供了一种可以让网络达到公共利益最大化的机制。



（图6：Aragon Network流程）

附录：Network服务

我们定义了AN组织需要雇佣的两个基础的网络服务，这些可能会或也可能不会由Aragon团队开发。下面不是协议的细节，而是我们研究AN需要的功能的简要介绍。

附录A：Aragon Network的去中心化仲裁系统

1. 驱动因素

在市场上进行交易时，会因为出现信任问题而导致股东之间的争论。多亏了智能合约无需信任的本质，许多表面问题没有了，因为条款可以事先约定，所以无人可以再事后取巧。但还有一些条款不能用代码描述，争论也就会随之而来。

我们思考下这两个例子：

- 一个投资人投资了一个组织并且有投票权。组织的创始人作恶并且把投资人所有的钱打到他自己的账户。如果这是个Aragon组织，投资人就希望可以规定，如果交易金额超过一定的上限，就必须经过更大范围的投票。
- 一个SaaS组织的创始人雇佣了一个的新系统管理员，然后雇主就可以有他们易受攻击的用户数据库的访问权限，就可以进行盗窃并用于私利。以太坊上运行的合约无法知道发生了什么，因此Aragon组织在处理人际间的信任问题时很无能为力。

我们相信需要有一个可以让参与者选择性加入的系统，来对抗这些人际行为。传统的解决方案是政府权力的仲裁。由于Aragon组织是运行在以太坊上的无政府环境中，因此我们想出了更好的方案。

2. 一个去中心化，透明的，可分叉的司法机关

一个Aragon Network Jurisdiction（ANJ司法机关）有如下几个合约功能：

- 提供两方任意争端的仲裁。
- 允许ANT持有者根据一些基本规则，对于将要发生的仲裁进行投票。

2.1. 实体

实体（比如组织或雇员）可以通过把他们的控制权交给司法机关的合约，而参与到网络中来。实体之间可以进行交互，例如一个组织和雇员可以用任何密码学的方式约定更多的细节（相比于智能合约里已有的），比如在某一时间，给一个共同的文件同时签名。

2.2. ANT在司法机关中的作用

- 对于众多决定的投票权，比如替换最高法院的一系列基本法则。
- 作为发起仲裁所需缴纳的押金。

2.3. 法官

想要参与仲裁的实体可以缴纳一个押金，之后就能充当法官。

3. 仲裁机制

为了发起一个仲裁，申请人需要缴纳押金，如果这个案子解决了，押金就会返回给他们，否则就会被拿走。

仲裁诉状可以引发冻结，也就是立即冻结被告的合约（比如一个攻击者正在利用一个漏洞）。只有发起人是被告组织的股东才可以提交这种诉状（图A）。

对于人类的裁判，法官的决定都分两步提交，来保证在做决策过程中的隐私化，而且不会影响到其他法官的决策。这种结构也用在了以太坊域名服务（ENS）的竞拍中，流程如下：

- 决定如何裁判后，法官会生成一个秘密的随机数，同时提交判决结果的摘要给法庭，之后保存好该随机数。
- 等裁判的期限过后，法官必须披露他们的随机数和判决结果，然后任何人都可以验证这个判决结果的。如果判决结果和随机数披露失败，会惩罚他们交的押金。
- 为了阻止法官勾结，如果任何人提前披露了某个法官的秘密随机数，那么这个法官就会被惩罚，而押金的一部分会给披露人。

3.1. 人类法官

当仲裁发起的时候：

- 从交了押金的法官中，随机选出5个。如果其中某个拒绝参加就会被轻微处罚，然后再选一个。
- 法官们看下ANJ的基本规则、该组织特有的规则、还有其他参与方加密后发送的材料。
- 他们提交判决结果，附带秘密随机数。
- 等待仲裁期过后，他们公布判决结果和秘密随机数。

- 押金会退给这些法官，外加把对败诉一方的处罚作为奖励。
- 投了正确票的法官会被奖励一些不能转账的声誉代币，而投错票的法官会被严重处罚。

3.2. 预测市场

如果申请人不满足那5个人类法官的判决，他们可以发起上诉（交更多的押金），网络中所有的法官都可以参与。对于这种情况，我们可以借鉴Augur或Gnosis。

当仲裁发起的时候：

- 法官们看下ANJ的基本规则、该组织特有的规则、还有其他参与方加密后发送的材料。
- 他们提交判决结果，附带秘密随机数。
- 等待仲裁期过后，他们公布判决结果和秘密随机数。
- 押金会退给这些法官，外加把对败诉一方的处罚作为奖励。
- 如果结果和第一次判决的不一样，所有上轮判决中投错票的法官都会被严厉惩罚。

3.3. 最高法院

如果申请人不满意前两轮的判决，他们可以继续上诉至最高级（交非常多的押金），然后由ANJ中最高声誉的9个法官组成最高法院。

当仲裁发起的时候：

- 法官们看下ANJ的基本规则、该组织特有的规则、还有其他参与方加密后发送的材料。
- 他们提交判决结果，附带秘密随机数。
- 等待仲裁期过后，他们公布判决结果和秘密随机数。
- 押金会退给这些法官，外加把对败诉一方的处罚作为奖励。
- 如果结果和第一次判决的不一样，所有上轮判决中投错票的法官都会被严厉惩罚。

这些法官会被支付由ANT持有者决定的薪水ANF（图B）。

3.4. 激励设计

看了上面描述的系统设计，你也许会争论说法官和整个网络会从经济激励上，不通过申请人的请求，然后他们就可以拿到他的押金来平分。

这也使申请人知道，如果他们的案子不够清晰就很可能会被否决。但法官也知道，如果他们撒谎或为了他们的私利而否决，他们的代币和押金就会被罚掉。

系统的设计是尽量不鼓励仲裁的发生，且尽量为被侵犯利益的群体主持正义。

4. 总结

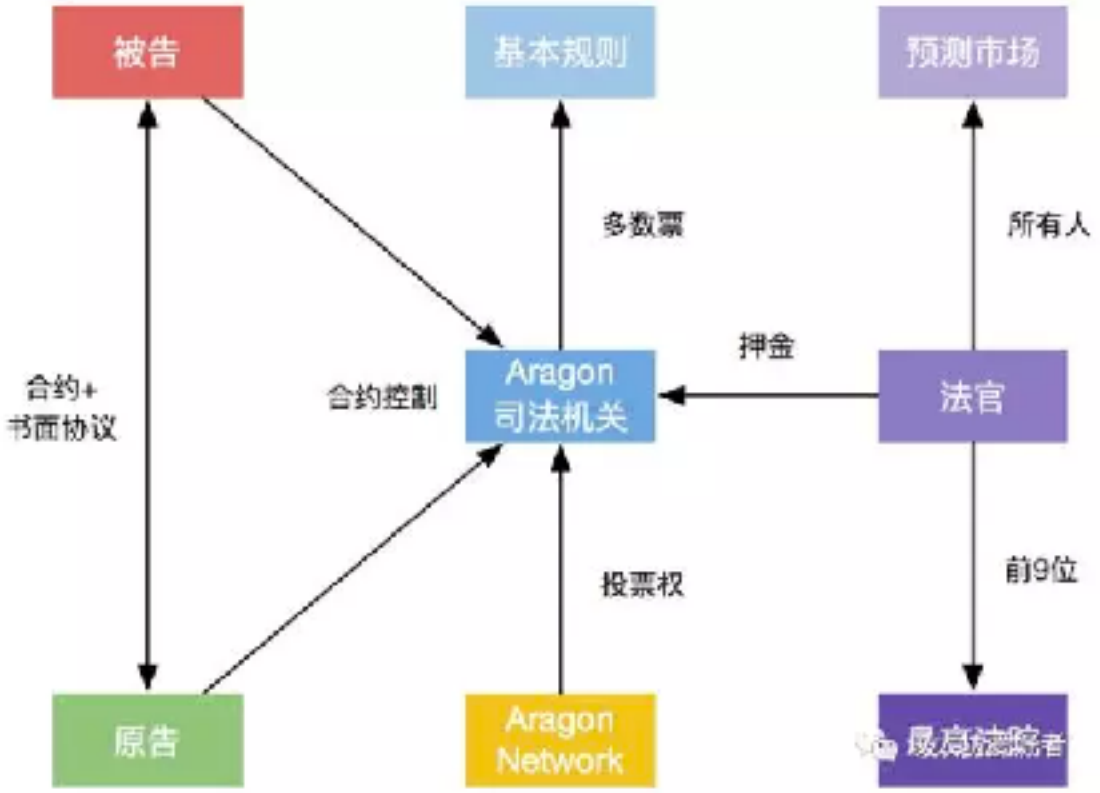
ANJ提供了解决人际主观纠纷的工具。它是Aragon组织激励机制的一部分，因为：

- 参与该组织业务交互的人们希望特殊的保证，以防合约有未覆盖到的信任漏洞。
- 通过提交一次仲裁，可以冻结一些有漏洞合约的全部活动，直到问题解决。

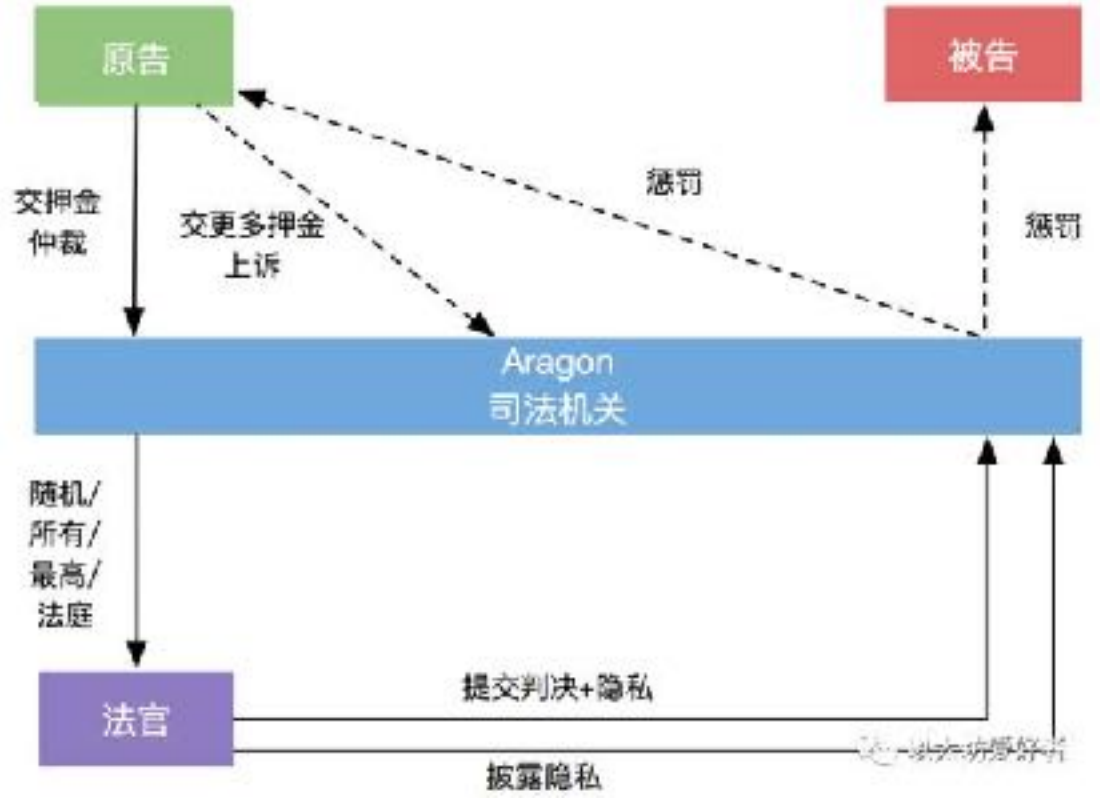
ANJ的投票流程是透明的，但在某些情况下，一些股东之间可能会分叉，这也激发了他们的治理模型产生作用。我们相信ANJ会创造显著的网络效应，因为：

- 和其他组织的交互也需要签约，因此引入更多可能的信任漏洞。

- 如果它是扩展的，那么所有参与方（包括投资人）都会熟悉它的基本规则。



（图A：仲裁流程）



（图B：ANJ激励）

附录B：Aragon Network的智能合约安全和升级策略

智能合约的最大的优势同时也是最大的劣势是：合约一旦被创建，就会永远在区块链上，而且永远按照开发者写的代码执行，然而那并不一定是合约创建者意愿的真实表达。
最重要的一个例子是The DAO被黑事件，一个预期之外的操作组合，导致合约转了很多钱给黑客。在这个案例中，被迫执行了一次协议级别的硬分叉来阻止资金流失。
我们创立Aragon是为了让人们可以运行DAO，从更广的范围考虑，也希望完全没听说过以太坊的人可以同样使用。
我们需要建立一个系统，让不熟悉细节的用户也可以确定性地运行他们的组织，并且他们可以永远运行软件的最新版本，尽可能不被攻击。
这个服务对于Aragon Network里所有组织的参与者都能用，但是组织可以决定多大程度上依赖它，从完全控制升级（必须经过组织授权），到完全自动升级（保证我安全，我什么都不懂），到中间状态（不要给我自动进行普通升级，只在有安全漏洞时自动升级）。
这个工作还在进行中，但如果我们希望成千的DAO可以安全运行，这就是个需要添加的重要的功能。

1. 组件

下面描述的是我们目前计划的保证网络集成度的几个不同组件。

1.1. 可升级智能合约的代理库

目前部署智能合约系统通常依赖一种人工代码安全性审计，部署到网络上后就只能希望它不会再出问题了。因为代码本质上是不可更改的法律，不可能用回退来升级，以修复几个漏洞或更好表达开发者的原始想法。

或者本身也不是智能合约作者的问题，而是由于协议的共识算法修改了，合约就变得很容易受到攻击。这会是个严重的问题，如果一个系统完全不能升级，而我们又希望今天写的合约会永远好用。这在简单系统里也许不是个问题，但对于Aragon Network里如此复杂的DAO组织来讲就是了。

我们已经调研了好几个月这个问题，我们目前的解决方案是尽可能多地把系统业务逻辑压缩到Solidity开发库中。做库驱动开发[J. Izquierdo, 2017]，然后不直接在合约里持久连接它们，而是使用代理调度[M. Araoz, 2017]合约，来让每个组织知道应该连接的库版本。我们在和最好的智能合约安全审计公司Zeppelin合作，来创建这个可升级库的代理系统，关于这方面我们最近也发表了文章。

这项技术还会使一些小组织的合约非常轻量，只有一些数据存储，然后跳转他们的逻辑到所有组织都在用的库里。

如果发现漏洞，一个新版本的库会被部署，然后网络内所有的组织根据他们的设置都会被

升级：

- 自动升级
- 通知升级，但需要授权
- 什么都不做，组织自行决定是否升级

1.2. Network范围的漏洞悬赏

让不同组织调用一个同样合约的负面效应是，他会引发黑客集中攻击。乐观的角度，也会让这些股东联合起来抵御攻击。
网络内会有一个漏洞悬赏计划，覆盖网络内组织需要调用的所有合约。历史表明如果人们在经济上被鼓励做好事的时候，大部分发现漏洞的人都会为了拿奖励而报告，而不是去伤害更多的人。
我们在考虑把漏洞悬赏做的自动化，比如为组织的合约写一个测试，如果有人可以打破测试，就会自动支付赏金。
网络的可升级机制也很适应漏洞悬赏计划，因为可以把从漏洞被发现到被解决的升级路径最小化。

1.3. 全网安全停机

如果一个服务漏洞被发现，Aragon Network可以停止所有组织的合约（如果所有组织都被牵连了），然后开展调查和代码升级，再重新恢复服务。

我们会开发一个机器人，它会监听所有发送到Aragon组织的公开交易，如果发现异常行为或非预期状态，就判断为有可能的黑客，它就会通知Aragon团队的人，如果机器人认为盗贼很恶劣，需要立即采取措施，它会停止所有的组织，再由负责的人了解情况。

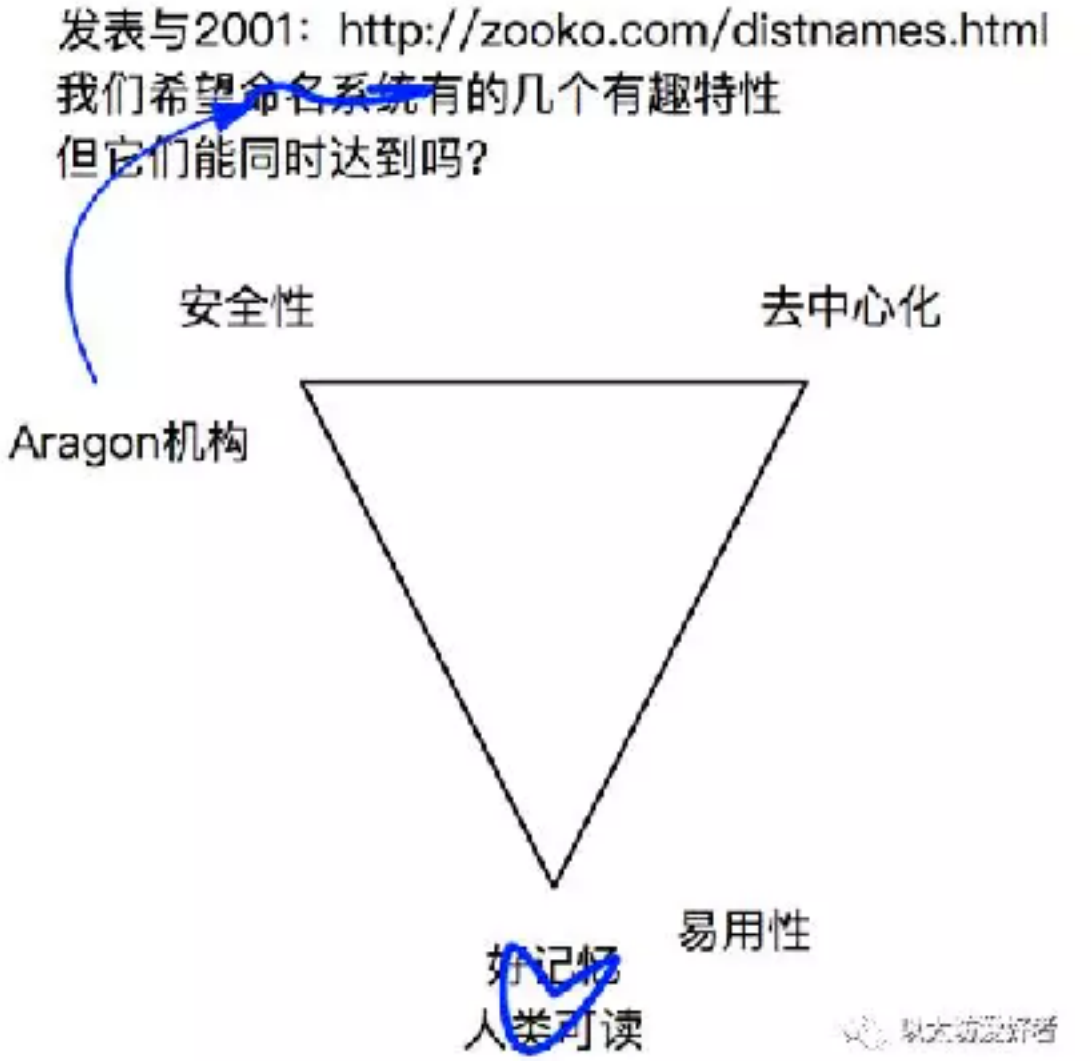
这意味着在30秒之内就可以停止一个对全体组织的攻击，升级后会立即修复。如果是错误警告，负责的人会重启服务，停机时间不超过10分钟。

1.4. 应对组织内恶意用户的司法操作

在上面ANJ司法组织的介绍里，网络内的所有组织都同意跟ANJ去中心化法庭所绑定。一旦一个案子被创建，法庭可以改变或撤销组织的操作。这个只是股东的一个防护措施。通过提供一个足够的押金，一个组织的股东可以提交一个诉状给ANJ，然后预防性地冻结组织。如果法庭决定这个诉状不合法，这个人就会失去他的押金而交给法庭（部分给该组织）

1.5. 权衡

跟生活中大部分好事情一样，安全性问题需要权衡。我们可以想象打造一个dApp的三角形，和Zooko的三角形（图A）很像，有安全性、去中心化、易用性为三个角，着重某一个肯定会疏远其他两个。我们发现三个特性都很重要，但也很难创造一个系统，让每个用户或组织可以任意选择他们愿意做哪方面的妥协。



A． 安全性

安全性的含义是及时解决漏洞和威胁的能力。

B． 去中心化

升级机制的问题在于最终还是由一个可信组织领导软件升级，这是非常中心化的。但网络可以选择添加一个投票机制，只有当代码被完全检查后才能发布升级。这也是我们的升级机制为什么是可选的原因，有些用户不想要这么高的安全性，而只接受对于自己组织的更新。

C． 易用性

如果把安全性和去中心化调到最优，肯定会降低用户希望理解Aragon来升级自己组织的易用性，造成很大的障碍。

2. 总结

有了以上描述的方法，Aragon Network可以保证：

- 将来的漏洞修复和增强可以添加进合约里。
- 由于漏洞悬赏计划、全网停机功能、和ANJ司法仲裁机关，严重的漏洞攻击会被最小化。

原文：Aragon Network Whitepaper
译者：岳利鹏（ethfans.org）