ETHERPARTY

用户友好型智能合约编译平台

KEVIN HOBBS k@etherparty.io
LISA CHENG l@etherparty.io
JEFFERY WALSH jeffery@etherparty.io
BRIAN ONN brian@etherparty.io

摘要： 用户友好型智能合约创建、使用及管理系统可能会极大地提高区块链技术的商业及消费者使用率。虽然区块链（或分布式账本技术）有可能重塑电子商务和数据存储的基础，但由于缺少用户友好的应用程序，该技术在非计算机专业人群中的使用受到了限制。Etherparty为个人及业务释放了智能合约快速、安全、低成本的优势。它代表了“软件即服务”的新世代。Etherparty承诺，它会像内容管理系统（如Wordpress和Wix）造福网页开发一样为智能合约带去发展。此外，虽然Etherparty类似于之前的Legalzoom和Docusign，但它会进一步使原本复杂的合约协议及流程更加简单且易于使用，同时启用验证和自动化的基础设施。

本文不属于任何形式的招股说明书。

本文件不构成或暗示任何形式的招股说明书。所有措辞都不应被解释为投资招标，本白皮书不得以任何方式与全球任何地区的证券发行相关。本白皮书是对Etherparty智能合约功能以及由Etherparty创建和发行的FUEL代币的技术描述。

内容

介绍

什么是智能合约？尽管智能合约的概念更加常见了，但普通大众对它仍然不太了解。这个概念最初由计算机科学家Nick Szabo在1990年代中期提出。他使用这个术语来说明可以把合同法和相关业务应用的先进部分用作陌生人在互联网上进行电子商务交易的设计。

Szabo 写道：“智能合约是执行合同条款的计算机化交易协议。其总体目标是满足共同的合同条件（如支付条件、留置权、保密性甚至执行），尽量减少恶意和意外的异常情况，并尽量减少对受信任中介的需求。其相关的经济目标包括降低欺诈损失、仲裁和执行成本及其他交易成本。”[1]

2014年，Vitalik Buterin在以太坊的白皮书中重新介绍了这个概念，随后由Gavin Wood在以太坊黄皮书中执行。文件表明，以太坊智能合约将通过以太坊虚拟机（EVM）执行，EVM是用于计算任意算法复杂指令的环境。这些指令以函数调用或信息的形式存在，可以使合约在网络上互动。目前存在的基本函数调用有160多种[2]，并且会随着以太坊网络向权益证明转变而扩大。[3]

我们相信人们对智能合约的需求会继续增长，因为自动化同侪互动或促进协调小组行动的应用程序[4]在日常社会中会变得越来越普遍。为了满足这一需求，Etherparty打算创建一个平台和增值服务，允许任何用户访问智能合约和区块链技术，不需要拥有这两方面具体的技术知识。

KEVIN HOBBS
CEO & Co-Founder
k@etherparty.io

LISA CHENG
Founder
l@etherparty.io

JEFFERY WALSH
Solidity & Full Stack Developer
jeffery@etherparty.io

BRIAN ONN
Chief Architect
brian@etherparty.io

1 Tapscott, Don; Tapscott, Alex (May 2016). The Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World. pp. 72, 83, 101, 127. ISBN 978-0670069972.
2 Go Ethereum 核心类型: https://godoc.org/github.com/ethereum/go-ethereum/core/types
3 globalRandao’和‘dunkle’是Vitalik的Mauve paper中提到的新概念: https://cdn.hackaday.io/files/10879465447136/Mauve%20Paper%20Vitalik.pdf
4 什么是以太坊: http://ethdocs.org/en/latest/introduction/what-is-ethereum.html

我们的方法

智能合同的主流使用将需要发明使区块链与更多传统技术（网页应用程序、公共API等）相结合的新架构解决方案。例如，可以在区块链上测试并部署的网页应用程序，用户可以通过我们的服务器在这个程序上注册并创建智能合约。我们这个产品目前的实施可以进行ERC20或ERC223代币[5]的创建及众筹，也允许两个用户对职业棒球比赛进行下注。

该应用程序使用两个托管的以太坊节点，一个用于实际的以太坊主网络，另一个用于测试网。这将允许用户在合约部署之前对其进行全面测试。在实践中，我们将部署多个负载均衡的以太坊节点，以处理预期的网络流量负载，并为Etherparty用户提供高度可用性。

这种网络应用程序的进一步发展将包括一个可供用户选择、不断增加的智能合约库，以及用户原创合约模板的市场。这将使非技术用户能够以智能合约的形式创建区块链交易，智能合约可以反映法律和商业环境中任何类型的协议。传统技术将继续提供追踪智能合约版本、平台用户名以及对应的登录电子邮件地址的方法。EVM将用于处理智能合约本身的托管和指示。

5 ERC20代币简介 -- https://www.coindesk.com/ethereums-erc-20-tokens-rage-anyway/

订阅模式

该应用程序提供分层订阅服务，第一层只能访问有限的平台功能，每个月能执行一到两个合约。第二层的合约限制少一些，而第三层会在上一层的基础上发展，限制更少，功能、流程和集成方面都更优越。合约将需要该平台的本地代币——FUEL。由于FUEL的价格可能会波动，我们将为合约设定固定的美元价格，并根据这个固定价格调整执行智能合约所需的FUEL数量。虽然当前的应用程序通过填写网页表单来工作，但我们希望为用户开发拖放界面，并使其通过自然语言处理创建智能合约。

我们将构建一个最初针对企业客户的公共API。这种API将允许企业保留现有的合同和流程，但会将其转化为智能合约，从而使这些流程得到区块链技术的支持。

我们的长期目标是成为“区块链不可知论者”。虽然以太坊拥有最先进的智能合约技术生态系统，但我们将与Rootstock[6]合作，使智能合约能够通过比特币创建。未来，我们将考虑把其他区块链集成到Etherparty生态系统中。

这些服务提供的是为用户节省大量时间和金钱的方式。使用Solidity——创建这些智能合约的编程语言，开发耗费时间和成本。寻找优秀的Solidity开发人员也很困难。构建基础设施来测试代码以发现漏洞是非常昂贵的。我们可以使您把这项工作外包出去。我们允许用户在测试环境中测试他们的合约，并对任何有漏洞的合约进行快速更新或重新部署，而无需额外的开发资源。智能合约的创建将和填写表单一样简单。

下一个进展在于采用

产品和应用程序要在全球范围内得到大规模采用，就必须使非技术用户和非行业用户也能接触它们。Etherparty计划在提供此类工具方面成为先驱，使下一波用户能够利用区块链和智能合约技术。

几乎每个人都知道如何使用电子邮件，但绝大多数人是通过服务供应商（如Gmail， Hotmail和Yahoo等）熟悉这项技术的。尽管很多人都可以做到这一点，但只有一小部分用户对电子邮件技术的了解达到了开发人员水平。这种例子在该行业中比比皆是，从网站开发到文档签名。因此，智能手机和智能合约技术也是这种情况。

Etherparty已经准备好了把区块链和智能合约技术提高到一个新水平。

安全性

人们对智能合约生态系统的主要担忧在于安全性。随着导致资金被盗的许多明显编程错误的出现，对安全性的担忧已经被推到了最醒目的位置。

Etherparty一直在关注这些问题，并创建模板，以减少它们出现的可能性。导致资金流失的常见问题，如使大多数标准ERC20代币深受其害的短地址攻击[7]，已经从你们的担忧变成了我们的关注点。

Etherparty定义了拥有分离存储合约的模块化架构，允许您部署的合约的功能随着智能合约的发展而升级，使您的数据得到维护。所有的合约都是从我们安全的基础模板开始的。

您在Etherparty平台上的以太坊地址的私钥存储在只有您可以访问的上锁保管库中。其状态管理符合当今最佳实践哈希标准。智能合约安全标准同样适用于平台本身，平台会一直处在监控状态中。

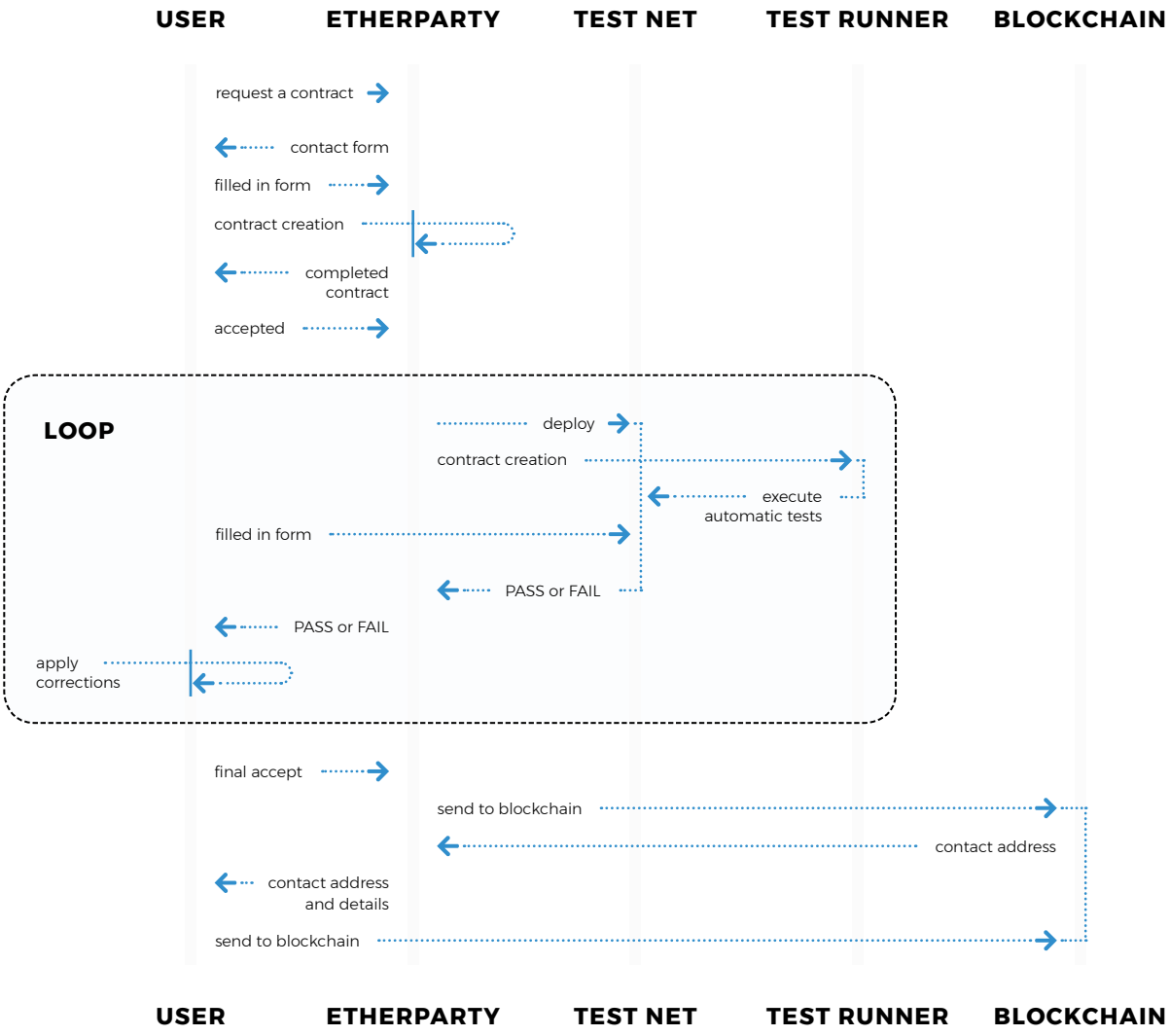
在目前的实施中，我们的以太坊智能合约使用最新版本的可用编译器在Solidity中创建。Solidity不同于Serpent[8]，提供了以太坊网络上最安全和最强大的编程接口。

我们计划在下一次迭代中部署监控工具以发现需要修补的合约，并启动简化更新的自动化程序。这将伴随着一种自动化测试服务，可以在合约得到部署前不断加强对它们的测试。

7 http://vessenes.com/the-erc20-short-address-attack-explained/
8 https://blog.zeppelin.solutions/augur-rep-token-critical-vulnerability-disclosure-3d8bdffd79d2

用户在可以部署我们的智能合约之前必须在Etherparty上接受尽职调查。这将防止我们的平台遭到滥用。我们格外关注发布众筹合约的用户，并且会采取额外措施确保Etherparty上的众筹合约遵循可接受的标准。

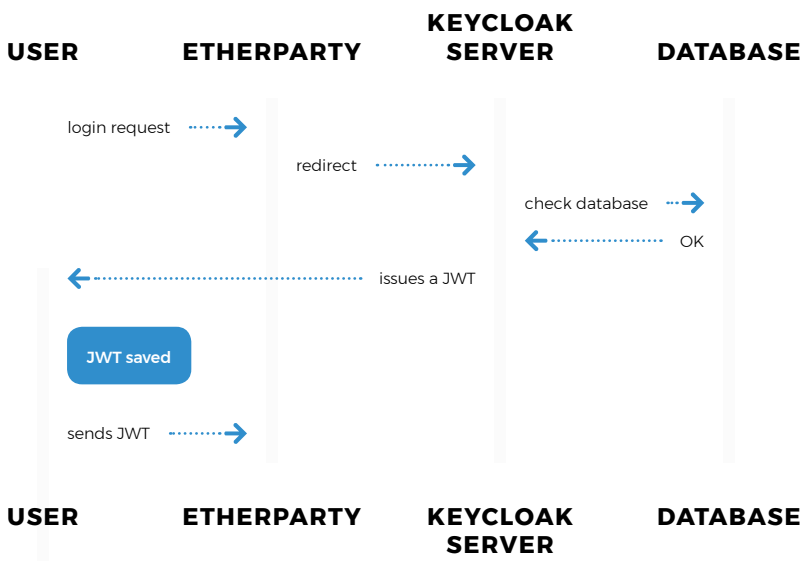
CONTRACT DEPLOYMENT SEQUENCE



平台安全

Etherparty的用户验证功能将完全由Keycloak服务器提供。这是一个知名的开源身份和权限管理（IAM）平台。Keycloak为我们的用户提供了安全保障，因为他们的个人数据会由当前最新的协议进行保护。Keycloak拥有同行评议特点，使用最佳用户身份及权限控制方法，并由开源社区持续更新以了解所有安全问题。

Keycloak支持双重认证（2FA）的特质使我们的平台能够和产品一样拥有高度安全性（并不是将来才能实现的）。我们也要求在任何可能出现价值交换的平台交易前或交易中通过Keycloak进行认证。这意味着用户会明白能够访问平台还不足以进行价值交换——必须再次认证，然后对自己在平台上存储的任何价值进行保护。



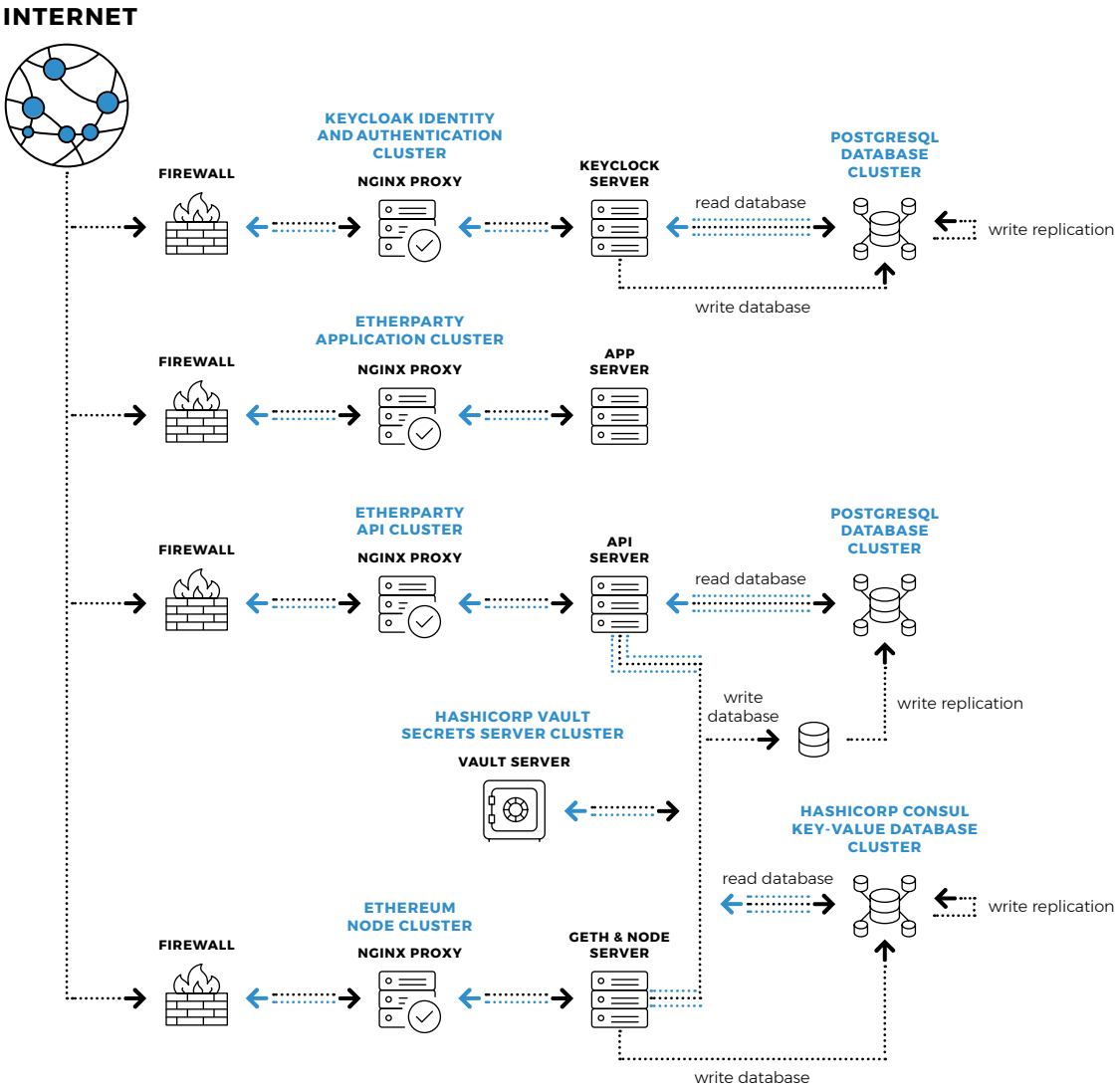
Etherparty平台会记录上一次登录的时间和地点，并且每次都将这些信息展示给用户。如果我们发现任何异常行为，比如使用新设备登录或从另一个地点登录，我们都会向用户发送邮件或短信通知，使其如有需要可以锁住账户。关键时，账户所有者可以直接锁定账户，因此在有人试图破坏时不需要Etherparty的支持人员。

该平台支持合法使用，也会在预料之外的异常行为出现时尝试自动锁定账户。为了实现这一点，我们会创建安全简历，并设置合适锁定账户的自动化决定，以进行调查。异常行为，如从可以地点登录，也会汇报给Etherparty的员工。

我们也会记录所有尝试登录失败的情况，并通过邮件将其汇报给用户。这样，用户就能及时得知情况并采取恰当行动保护其账户。

Etherparty平台也会使用现有的最佳方案识别攻击和“账户盗用” （ATO）企图，并在账户被盗走之前将其锁定。

ETHERPARTY NETWORK ARCHITECTURE



仲裁

在进行合约结算时，用户可能需要来自第三方数据源的信息。目前，这是与之相连的仲裁第三方API的工作。由于智能合约的使用在向企业和日常用例扩展，合约处理的自动化将需要第三方数据源。如今已存在的链上方式要为第三方数据源[9]创建概念系统。当我们与受信赖的数据源合作时，该方法非常有价值。

我们的方法必须考虑到受信任的数据源可能在将来某个时间点发起恶意行动的后果。因此，我们将要求对直接输入区块链的数据进行链上验证。这个信息需要反映在合约的输入功能中[10]，但仍不能证明信息是否可信。我们希望接下来的研究可以解决这个问题。

9 Oraclize.it
10 https://ethereum.stackexchange.com/questions/11589/how-do-oracle-services-work-under-the-hood

用例

智能合约的应用非常广泛。Etherparty平台将创建一个智能合约库，以服务于多个行业，包括银行和金融业、贸易、医疗保健、供应链管理、保险、外汇交易、房地产、数字身份等。智能合约将在这些行业得到应用，因为它能通过自动化减少交易摩擦和成本的合约协议提供实质性好处，同时加强数据安全。任何类型的合约都可以通过使用智能合约技术得到改善。

为了介绍Etherparty智能合约将如何解决多种现实世界问题，我们进行了以下行业的研究汇总：

金融服务

> 里程碑式支付变革
> 托管

问题: 与另一方一起管理付款流程可能会导致差异、错误和混淆的出现。无论是个人协议还是商业合同，都可能出现错误、不一致和文件丢失的情况。

解决方案: 智能合约用明确的规则将双方联系起来，按照书面规定发挥作用，消灭了出现不同意见的可能性。Etherparty会进行安全处理，以确保您的合约不容易被篡改，并提供完全可信的付款流程。

制造业

> 供应链管理
> 贸易金融

问题: 鉴于价值链的各种复杂环境和对纸质文件系统的依赖，追踪物品和信息是个麻烦且漫长的过程。这个问题在跨国追踪的情况下更为严峻。

解决方案: 有了Etherparty的企业API，将任何信息系统整合到平台上都会变得简单方便。编写智能合约会使各方处于同一个共享账本（区块链）上，这对于参与其中的各方来说都更加快速、安全且透明。

跨行业

> 点对点交易
> 承包商协议
> 具有可执行条件的合约（例如智能遗嘱认证或智能遗嘱）
> 记录保存

问题: 从两个公民间的简单赌注到数据记录的维护，互联网已经把商业互动转化为数字化安排。

解决方案: 智能合约和区块链技术可以减轻对违反合约或数字记录真实性的担忧。Etherparty通过设置恰当的条款使人们能轻松创建智能合约，它将自动执行各方概述的协议。此外，智能合约可以通过哈希把记录放到区块链上，从而消除数字上传的任何歧义。

法律

> 创办业务
> 公司申报
> 股息
> 监管链

问题: 文件丢失、不确定某些内容是否已经申报、处理敏感文件时的信息缺失。

解决方案: 在共享账本中存储业务创办和公司申报信息，这些信息不可更改且没有争议，且文件的授权和访问也会被记录。

进行ICO

> 众筹
> 代币创建
> 观察进展

问题: 安全性测试中的错误，部署需要以太坊服务器且要熟悉命令行。

解决方案: Etherparty提供部署解决方案以及与合约互动的GUI。所有合约均经过安全性测试，符合最新安全标准。

FUEL代币

FUEL代币是使用Etherparty的关键，它们管理合约库、安全性测试、网络手续费、监控及整个智能合约流程。

FUEL是一种部署在以太坊网络上的可传输ERC-20数字代币，是为Etherparty平台提供动力的应用内货币。用户将使用FUEL获得访问权限，从而使用平台的功能。FUEL代币是验证用户与Etherparty互动的方法，允许用户在平台上购买，执行或交换其他智能合约。未来，FUEL将作为多个区块链上智能合约的访问权限，把不同的区块链集成到Etherparty平台的统一视图中。

FUEL代币的总供应量为10亿，且不会再增加。FUEL的最小单位是 wei[11]。在平台上使用的代币会再次回到平台供应中去。我们将为用户提供从这些供应中购买FUEL的服务。

> “ FUEL代币是在不同行业和平台创建智能合约的网络代币。

11 一个wei是10-18

THE ICO

此次ICO将使我们能够聘请新员工，进行营销及业务和产品开发，这样我们才能成为市场上首个任何人都可以使用的智能合约平台。

分配

FUEL代币的数量为10亿，其分配计划如下:

> 40% (4亿) 的代币将在预售中面向符合SAFT[12] 供应的买方或通过公司认可的相关机构出售。如果所有的预售代币都以35%的最高奖励水平卖出，那么总共会售出5.4亿FUEL代币。

> 40% (4亿) 的代币将在正式众筹中出售。如果预售中的代币以35%的最高奖励水平全部卖出，那么只有2.6亿代币可用于公开销售。

任何预售中未售完的代币都会用于公开销售。

所有公开销售中未售完的代币都会留在Etherparty平台上，仅在平台上售出，最低价格为1美元。

> 10% (1亿) 的代币将由公司保留，用于激励社区、测试者和战略合作伙伴。

> 5% (5000万) 的代币将在平台上以最低1美元的价格直接出售。

公司持有的Etherparty平台代币的价格将为1美元或最高交易市场价。

> 5% (5000万) 将被分发给Etherparty团队。

Etherparty平台和公司员工的代币将在众筹结束后被锁定6个月。

12 https://coinlist.co/about/help/saft

预售

预售于2017年9月15日结束，或者是当预售份额全部售出为止（日期可能有变）。公司在预售（早于正式众筹）中向大批量购买者提供折扣优惠或通过授权相关机构进行:

> $50,000USD + 15%奖励

> $100,000 USD + 35%奖励

请联系 K@etherparty.io 了解预售详情

公开销售

FUEL代币预计按以下价格出售:

第1周: 1 ETH = 3000 FUEL

第 2周: 1 ETH = 2250 FUEL

第 3周: 1 ETH = 1700 FUEL

第4周: 1 ETH = 1275 FUEL

*注意 公开销售开始前，ETH的价格可能会变化。一旦公开销售开始，其价格将被锁定。
**注意 预售的价格不变且会一直保持原样，对公开销售没有影响。

附录

Etherparty的未来发展及发布时间表 *

第1项发布

(2017年第四季度末)

后端系统

- 从Firebase数据库后端向Postgresql转变
- 为合约平台创建安全的REST(Representational State Transfer 表述性状态转移)API，使其作为PaaS（平台即服务）得到采用，从而获得稳定的订阅收入
- 开发更多的REST API功能，以支持供应链管理
- 通过Docker container降低部署难度并提高可扩展性
- 遍布应用程序服务器的微服务架构和JSON网络代币
- 包含服务器关联性的网页服务器代理
- 用于部署的拥有合约库且受全面管理的区块链DAPP模式

前端系统

- 使用Web3 SSO（single sign-on单点登录）为平台创建不用点击的Web3登录
- 使用Metamask
- 双重认证 (2FA) 及合适的身份和权限管理 (IAM) 解决方案
- 上次登录的地点及时间
- 进行任何转移价值的活动时都需要更多的安全检查

认证与授权

- 使用经过公开审查的已有开源IAM服务器（如Keycloak）或者经过验证的云端IAM 服务（如ForgeRock，Stormpath或 Okta）
- 通过2FA加强登录安全
- 防止用户ATO（account takeover 账户盗用）欺诈的解决方案

网络组织

- 多层负载平衡和监控
- 使用ehcache或memcached产品的数据库和后端服务间的分布式缓存层

云端

- 用于管理Docker container的Google Container Engine (https://cloud.google.com/container-engine/)和Kubernetes (https://kubernetes.io/)或Mist.io (https://mist.io/)，Red Hat Openshift (http://openshift.com/)，或由Kubernetes支持的类似云平台
- 联合ElasticSearch，Graphite或Prometheus提醒人们注意超出特定范围的运行数据
- 联合Slack，Skype，BigPanda和/或PagerDuty发布通知

*注意　所有发布时间和发展分类都只是预估的，可能有变动。

13 http://vessenes.com/the-erc20-short-address-attack-explained/

14 https://kubernetes.io/

15 https://mist.io/

16 http://openshift.com/

第2项发布

(2018年第二季度末)

移动应用程序

> 推送通知

> 为Android和iOS提供全面的移动设备支持

通知

> 交易历史记录

> 平台上的桌面通知

> 平台下的短信通知

> 与短信应用程序合作发布通知

合约模板及合约库

扩大合约库，使其包含:

> 具有法律约束力的合同

> 投票和民主选举合同

> 公证服务

> 多人托管合同

> 家族信托

> 金钱管理

> 公司股票

> 虚拟民主

> 众筹

> 分时使用

> 定时锁定保险库

> M of N (多重签名)托管

> M of N (多重签名) 保险库

> 房产销售

> 供应链管理需求

预言机系统

> 与第三方API相结合的服务器

> 提供选择的API市场

*注意　所有发布时间和发展分类都只是预估的，可能有变动。

第3项发布

(2018年第四季度末)

前端系统

> 拖放合约创建功能

移动应用程序

> 与 Android上的 Google Assistant 结合

> IVR（interactive voice response 互动式语音应答）

> 企业集成功能

> 为企业客户开发更多REST API功能，使其能够在团队中添加用户，创建合约模板，在我们的测试网络上测试合约，把合约提交给主区块链并使合约发挥作用

企业解决方案

> Etherparty的高级用户界面拥有更多对企业客户来说十分必要的功能

> 用户原创模板

团队及团队特点

> 增加团队成员，分享并注释合约，合作创建新的合约模板

*注意　所有发布时间和发展分类都只是预估的，可能有变动。

ETHERPARTY

KEVIN HOBBS
CEO & Co-Founder
k@etherparty.io

LISA CHENG
Founder
l@etherparty.io

JEFFERY WALSH
Solidity & Full Stack Developer
jeffery@etherparty.io

BRIAN ONN
Chief Architect
brian@etherparty.io

ETHERPARTY
300-717 W Pender, Vancouver, BC, V6C 2X6

www.etherparty.io