YOOBA

去中心化的基于区块链的电子商务系统

叶松 (fly31318@gmail.com flyye@yooba.org)

2018.3.13

官网：https://yooba.org 邮箱：yooba@yooba.org

目录

1 起源

互联网的出现使人们的生活发生了翻天覆地的变化。人们的生活越来越丰富 ,越来越便捷。使用互联网消费满足日常需求已经成为大多数人们的生活习惯。现在衣服，家具，零食，书，游戏，车，房等几乎所有实体物品或虚拟物品都可在网上获得 ,甚至很多服务只能通过互联网才能获得。大大小小的网站数不胜数，提供的服务更是包罗万象。发展过程中也出现了一些问题和矛盾。

作为消费者，用户需要在多个不同大大小小的网站上注册，提供不同程度的个人信息，需要记住多个账户密码，不同服务商提供的服务体验和质量不尽相同。不同服务商对用户信息的保护意识和措施也是千差万别。用户数据可能一处泄漏造成多处泄漏。用户数据泄漏或数据用作何种用途，用户基本不能控制甚至不知情。

作为服务商，由于数据竞争、资源竞争、用户竞争，逐渐形成了数据寡头，资源寡头的局面。这些寡头像龙卷风似的吸纳了越来越大的范围，逐渐形成了行业主导者和规则制定者。新进者难以入局或做大。最终影响了用户的服务体验和服务多样性。

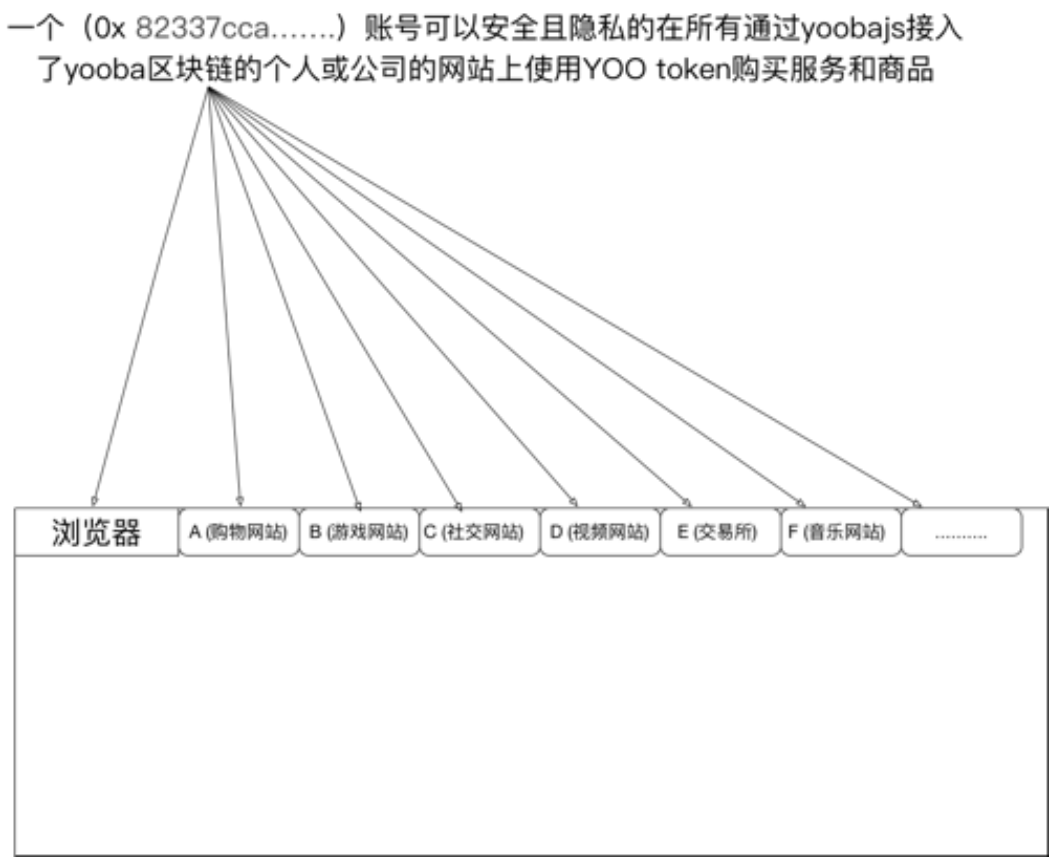
Yooba 就是解决上述问题的方案。Yooba 致力于让所有消费者，通过一个账号安全、隐私、自由、方便地进行全球性的消费；致力于建立一个全球性的，去中心化的，透明的，公平的，具有活力的商业平台。当然这是一次实验，可能成功，也可能失败。

2 .Yooba 应用场景

Yooba 是只为购物而生的区块链系统。虽然她可以应用在方方面面，但是 Yooba 的研究、发展及维护只围绕商品和服务有关的商业场景及未来。以下简单列举一些应用案例。

2.1 随时随地分享/售卖/发现商品和服务

任何用户或企业可以通过 App、pc 钱包上传自己的商品（包括常规商品，艺术品，二手物品等）或服务（包含知识、音乐等虚拟产品）。某些主体网站可以通过 yooba 收集这些中感兴趣的商品或服务并分类，形成各类服务网站。用户只需一个 Yooba 账号，一次登录（浏览器插件登录）就可在所有接入 Yooba 服务的网站获得服务。如下图



2.2 大超市平台

具有较强信誉的主体或平台可以在 Yooba 上建立大平台大超市，在 Yooba 上选择其信任和可控的小公司或个人拉入他的商店。他们通过 Yooba 建立了虚拟的组织关系。通过这种方式可以组成各种复杂的商业组织形式。

2.3 供应链

小到一个玩具，大到一辆汽车，它们的各个组件都可以在 Yooba 找到。任何人都可以公平透明地在 Yooba 上去选择自己所需的性价比最高的组件。Yooba 完整记录了供应链的供求关系。及它们的交易历史。

2.4 保险

不同的商业场景有不同的风险与不同的安全策略。保险即是 Yooba 中的一项基础服务（由不同服务商接入提供），也是一项很大的生意。

2.5 存储、人工智能等

Yooba 上大量的商品数据，交易数据等为存储、大数据分析、人工智能等提出了更高的需求并提供了更广阔的前景。任何公司主体或个人可以公平地获取 Yooba 上的商品，公开的交易记录，用户，商店等可见数据发展自己的业务，并在 Yooba 上或其他地方提供服务。

3 Yooba 设计思想

3.1 本质

Yooba 的本质是一个区块链。她的目标是让所有消费者，通过一个账号安全、隐私、自由、方便地进行全球性的消费；建立一个全球性的，去中心化的，透明的，公平的，具有活力的商业平台。所以它的设计、社区发展、应用推广均会围绕这个目标。

3.2 需求

- 高性能：几十甚至百万级每秒的交易处理速度以满足全球用户购物体验
- 低延迟：秒级的确认速度，提高交易体验

- 大存储：丰富的商品和服务所需要的巨大的存储空间
- 高扩展性：各种商品交易场景所需要的不同交易流程和规则，自由地接入第三方服务，网络。满足各种商业模式
- 去中心化：各卖家、服务商、商业主体利益冲突明显，需要有公平透明的机制维护，并无中间人控制
- 安全、隐私：极大地保护用户隐私及财产安全

3.3 区块链介绍

区块链发源于比特币，因其去中心化、分布式、去中介、不可串改、可编程等特性，对各行各业具有极大的颠覆力量。区块链的核心是去中心化，多个对等节点共同维护、发展这个公共账本。任何节点或中间人很难甚至不可能根据自身利益去控制一个开放的运营良好的区块链网络。

区块链是伟大的，它的出现有其必然性。公平、正义、自由、个性化在人类长河中经常作为信仰或理想被人们所追求。区块链的去中心化、不可篡改、DAO等特性某种程度上体现了这些特性，满足了大多数人的内在需求。

3.4 Yooba 实现重点

Yooba 并不打算完全从头实现一个自己的区块链系统。当然那样做也有其优势，但是我们的人力物力等资源有限。我们选择站在巨人的肩膀上。我们选择的是目前区块世界中技术和应用相对比较成熟的以太坊(Ethereum ,向 Ethereum 表示感谢，感谢他们为区块链为世界所作的努力和贡献)。Yooba 会对其进行改造以适应自己的需求和目标。当然我们也不打算长期活在以太坊的阴影下，我们

不希望 Yooba 的发展受限于以太坊的技术发展（毕竟我们的目标不同）。Yooba 会一步步的改进甚至替换掉以太坊的核心组件，只要它不适应、约束了 Yooba 的发展，我们就会这么做，当然我们也会尽力保证 Yooba 的兼容性。逐渐地 Yooba 会形成自己的一套完善的技术体系，以最大限度地支持自身的发展场景。

3.4.1 账户体系

Yooba 是为购物，为商业而生。根据其应用场景，Yooba 上有 3 种类型的账户：Account，Store，Contract。但相比于以太坊 Yooba 对账号结构和能力上进行了扩展，以适应 Yooba 的应用场景。

Account

```
type Account struct{
    address
    balance
    homepage
    score
    goodsurl
    historyurl
    ordersurl
    ...
    ...
    ...
}
```

Account 是 Yooba 的基本类型账户。大多数消费者的账户类型都是 Account。Account 可以进行通常的交易，创建智能合约（Contract），投票，上传商品/服务，下线商品/服务,买卖商品/服务。从上面的 Account 结构体中可以看到，Yooba 中的 Account 除了 balance 属性外，还引入了 homepage、score、goodsroot、historyurl、ordersurl 等。下面给与简要介绍。

- ✧ homepage(主页)，为 Account 个人或商店主页。这个主页默认为 https://explorer.yooba.org/address/Account.address 但是用户可以自定义此地址（例如自己的官方网站）。
- ✧ score 信用分。此分数由根据 Account 在 Yooba 上的交易记录和历史评价计算获得，并且全网同步。Score 初始分 5 分，满分 10 分，最低 0 分。Score 影响用户对其商品，服务的信任度，从而影响用户在 Yooba 上提供的服务的受欢迎程度。同样也影响用户在 Yooba 上所能享受到什么服务。例如某个服务提供商在其提供服务的智能合约中进行限制：只有 score 大于 7 的 Account 有权购买此服务。Score 具体计算机制在 Yooba 的初始版本中不会实现。在未实现之前其值为 5。不排除在某个版本实现 Score 时会利用已经存在的历史记录作为初始化 score 方式。
- ✧ goodsroot 是 Account 商品列表的 hash 根，可以用来检测商品是否更新，及索引存储在 IPFS 上的商品列表。
- ✧ historyurl 和 orderurl 根据 Account.address 自动生成。使用它们可以检索 Account 的商品交易历史信息和 Account 的订单信息。 这些信息也是存储在 IPFS 上。历史记录和订单需经过授权的 Account 才能查看，具体的授权机制使用智能合约实现。

Contract

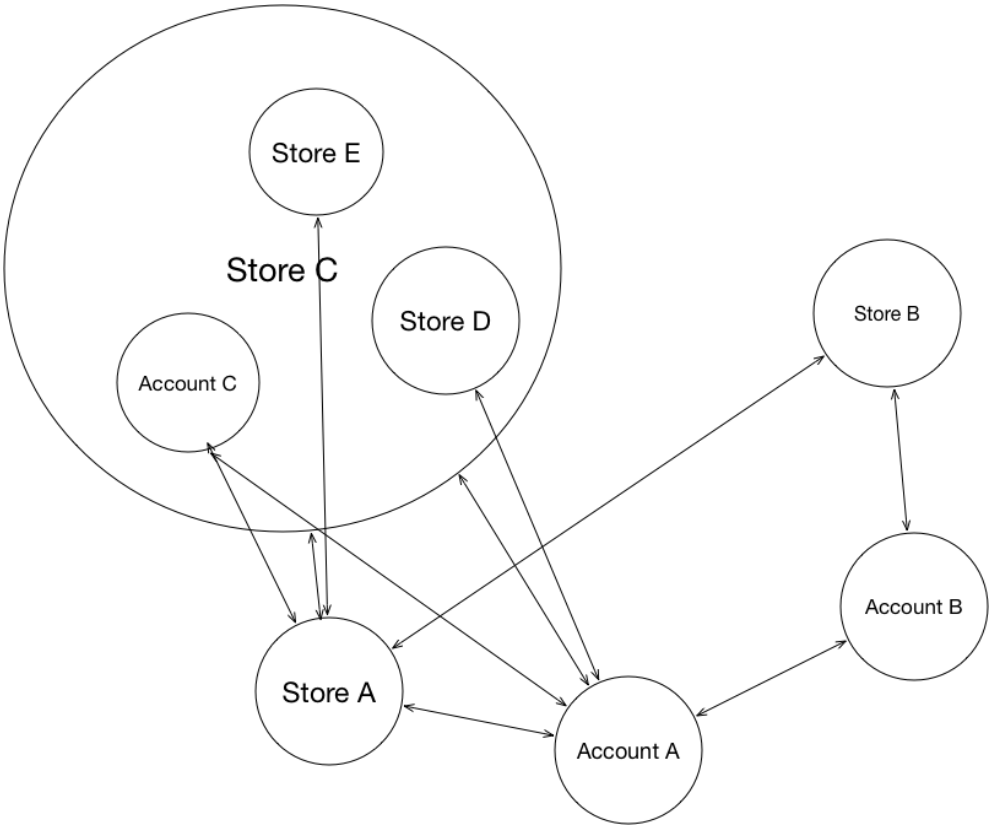
Contract 是智能合约。智能合约是一串完成特定功能的代码集合。它能够运行于每个节点上的虚拟机。由于编写 Contract 的语言是图灵完备的，Contract 可

以实现非常多各具特色的应用和功能，只要想象力足够丰富。在以太坊上 Contract 就被广泛地应用于代币的发行。当然 Yooba 中智能合约主要并不是用于此，它能够作为交易的前置条件或后置条件保障交易的顺利进行。它还可以作为广大虚拟产品的载体以商品的形式进行买卖。如游戏币，限时使用产品（影像产品，知识产品），保险，即时服务等等。Yooba 交易的隐私性也由智能合约提供（后文详述）。

Store

Store（商店）在现实生活中，无处不在。在 Yooba 中 Store 的位置同样重要。Account 就像生活中的个人，Store 就像现实中的商店，公司等组织。之所以把 Store 和 Account 分开，是因为 Store 在 Yooba 中的意义和 Account 有太多的不同，并且在 Yooba 后续的升级中 Store 经常会被加入新的特点以满足系统的不断发展和完善。

Store 的结构和 Account 的结构类似。也拥有和 Account 类似的功能。但 Store 中的商品可以来源于其他 Account 或 Store。就像现实中的大超市有很多的货源供应商一样。Yooba 中 Store 包含进其它 Store 以形成一个大的 Store。下面说说我们为什么要设计这么一个功能！



我们都知道信任在交易中的作用非常重要。通常情况下正规的卖方不介意买方是谁，只要收到钱，就会提供服务或商品。而买方往往要求对商品和卖方有更多的了解，才能放心的将钱交出去。通常买方希望尽可能的保护隐私，而卖方希望尽可能的推广自己的品牌。买方的根本诉求是把钱交出去买到好的商品，至于自己的真实姓名，性别，年龄，身份 ID，电话号码，买的什么东西等等信息卖方知道得越少越好。在 Yooba 上用户只需要向商品合约输入正确的参数，并向其转入商品价格的 token，就可获得相应商品或服务。卖家只知道有人购买了他的商品，以及将商品寄往何处或哪个账号接收商品。其他关于买家的信息根本不需要知道。所以卖家通常是愿意将自己的信息告知用户。而买家一般不会信任不认识的个人或者不知名的小团体，在缺乏第三方担保的情况下，偏于谨慎的用户一般不会去购买他们的产品。所以就算有很多个人 Account 上传了商品，对于普通用户来说购买他们的产品依然是一种冒险。因为用户可能给了钱，却收不到产品，

还找不到商家（商家提供的信息部分有假）。但是总会有一些用户愿意去购买他们的产品。 如：商家的熟人，通过线下确认其身份后，同城线下送货，为了稀有的产品愿意冒险的用户。我们希望有更广泛的用户可以享受到 Yooba 的服务。Yooba 提供 Stroe 账号类型来尽可能地提供更优质的服务和吸引更广泛的用户和商家。

假设一个非常知名的品牌，通过 Yooba 客户端创建了 Store 账号，并上传了自己的产品。然后它在自己的官网上（可信的地方），通过 Yoobajs 接入 Yooba 服务，登录其 Yooba Store 账号，就可将其 Store 账号里的产品展示在其官网上（当然展示页面需要自己定制实现），这样用户就可以非常相信的用 Yoo token 购买其商品，因为其官网是可信的。这种方式推广下去，用户就可以登录浏览器的 Yooba 插件后，浏览到哪里（游戏网站，音乐网站，视频网站，购物网站等）就用 token 购买就行了，不需要登录其他暴露隐私的账户，购买更方便更快捷。

再假设另外一种场景，另外一个知名购物网站，想增加更多产品,建成一个大的平台。这些大型的平台型 Store 又可以加入很多当地可信的个人和小 Store 进去。这些大型的 Store 可以有自己的对在自己平台内的小 Store 的身份认证机制。他们有责任和义务去筛选他们的服务商以保护用户的利益。因为对外用户看到的是大型 Store，对内他们会按照合约收取平台内商户的一定费用。另外这些大型的 Store 又可以引入保险等服务商增强他们的信誉度。

这些大型的服务商，保险，物流，合约等某种程度代表了一定的信任中介。这样在去中心化的系统中，通过各个可信环节，相对可信的 Store，可信的服务商，可信的步骤等一步步来增强交易可信度，来更好的服务用户。并且这些相对可信点不是相对领域的唯一点，所以不会导致领域性中心化。并且各个点是相互

竞争关系，有利于提供更好的服务。

3.4.2 隐私

隐私一直是用户非常在意的功能之一。资产、交易记录、个人信息等对用户来说非常重要。因为掌握了这些信息，掌握了用户的消费习惯、行为特征等。没有人愿意完全的暴露在另一个人眼中，更不用说暴露于公众之下。个人的数据应该由个人掌握。任何第三方都不能保证 100%的数据安全和不滥用数据。我们应该将自己的东西握在自己手中。

加密货币领域隐私性较高，应用较为广泛的有零知识证明（ zk-SNARKs)和环签(Ring Signatures)。对应的知名项目为 Zcash 和 Monero。

- Ring Signatures 环签是一种数字签名，可以由用户组中的某人用其私钥进行签名。但是不暴露谁在签名。也就是说无法将 public key 和签名绑定起来。当参与环签的 public key 的数量越多，隐私性越高。当然其使用的成本也越大。
- zk-SNARKs 允许证明者向验证者证明其陈述是真实的，并且这个证明不会泄露超出陈述本身有效性之外的任何信息。使用零知识证明可以保证交易双方、交易什么等信息不会泄露。

由上我们看到 zk-SNRKs 具有更高的隐私性。但是生成零知识证明非常耗费资源。目前在 RAM 3G~4G 以上的性能相对不错 PC 上生成一次证明需要 40 秒左右。这显然限制了其在手机上面的应用。相比之下环签具有更高的性能和体验。不过根据 zcash blog 介绍 zcash sapling 升级将会极大的降低零知识证明生成所需要的资源和时间（时间会降低到秒级，内存降低到 40M 左右)。所以零知识证明

在移动端上未来也将发挥更大的作用。

Zcash 和 monero 等大部分加密货币是在区块链底层实现的隐私保护。以太坊已经在探讨和实现智能合约层的隐私保护机制。Yooba 为了更大的自由度，更广泛的应用场景，也选择在智能合约层实现隐私保护。Yooba 会实现、提供多种隐私保护的智能合约作为基础模块供用户选用，其中就包括环签和零知识证明。

3.4.3 DPOS

Yooba 就是为购物而生。这其中的交易不仅仅包含代币之间的交易，还包括各种实物和虚拟物品的交易。这就对系统的处理能力提出了很高的要求,并且要求很低的确认延迟及很低的交易费用。Yooba 选择了 DPOS 这种满足这些要求的共识算法(不排除后续更新更为优秀的算法)。所有拥有 YOO token 的 account 都有对应比例的选票用于选择哪些可信的节点作为记账节点。相比于 pos，代理权益证明机制（DPOS）减少了有大选票权的用户直接参与作恶的可能性，也分散和降低了他们的权利，让整个系统更加的去中心化。

Yooba 的记账节点为 31 个。Yooba 的每一轮选举首先选出 51 个初始记账节点，然后再在这 51 个中随机选择 31 个作为本轮胜出节点，作为记账节点。

3.4.4 存储 IPFS

Yooba 发展到一定阶段，会成为世界型的购物平台和交易平台。包括图片，商品介绍，交易时的交流信息等很多信息是即时的或个人相关的，并且数据量是庞大的。这些数据不应该永久存储或保存在全局的区块链上。但这么多信息存储在哪呢？既能保证商品信息的安全性，又能保证数据需要时不会找不到？这里我

们先看下 ethereum 的 swarm。swarm 是一个优秀的分布式存储方案。它利用各个节点上运行 swarm 节点占用节点所在设备的一小比例空间（或者云空间）用于存储。所有这些小块空间组成一个巨大的空间。但 swarm 有其局限性。swarm 各个节点的出现和消亡是频繁变化的。一小段时间内可能就有上万的旧节点消失和上万的新节点出现，就会出现频繁的数据更新和迁移。再者 swarm 不适宜存储较大的数据，swarm 会将数据或文件拆分为 chunk 存储，而每一个 chunk 最多存储 4104 字节的数据，swarm 主要用于存储合约代码和区块链数据。由于 Yooba 中商品相关信息这些数据量比较大，且文件单体比较大，不适宜做频繁的迁移。我们使用 IPFS 作为 Yooba 主要的数据存储方式。

IPFS 上是一种内容可寻址、版本化、点对点超媒体的分布式存储、传输协议。Yooba 上 Account 的 goodsroot,historyurl,orderurl 所指向的地址就是 IPFS 地址。用户的数据在 IPFS 上是加密保护的，只有经过授权的用户才行访问和解析数据。用户需要为自己所使用的存储空间进行付费（使用 YOO 支付）。具体的费率是动态变化的。存储服务商也可以加入进来提供稳定的存储服务，从而获得报酬。用户所使用的空间在欠费达到一定额度时，其所使用的空间会被释放。当然用户也可以主动删除部分商品减少存储和节省开支。

4 社区发展计划

Yooba 的发展壮大必须依靠社区的大力支持。Yooba 为了避免代币集中化，同时也为了吸引目光，刺激项目初期快速发展，Yooba 将拿 20%的代币进行空投。预计空投完成时，将会有 10 万~20 万的用户拥有 Yooba。这给了 Yooba

发展强大的初始动力。

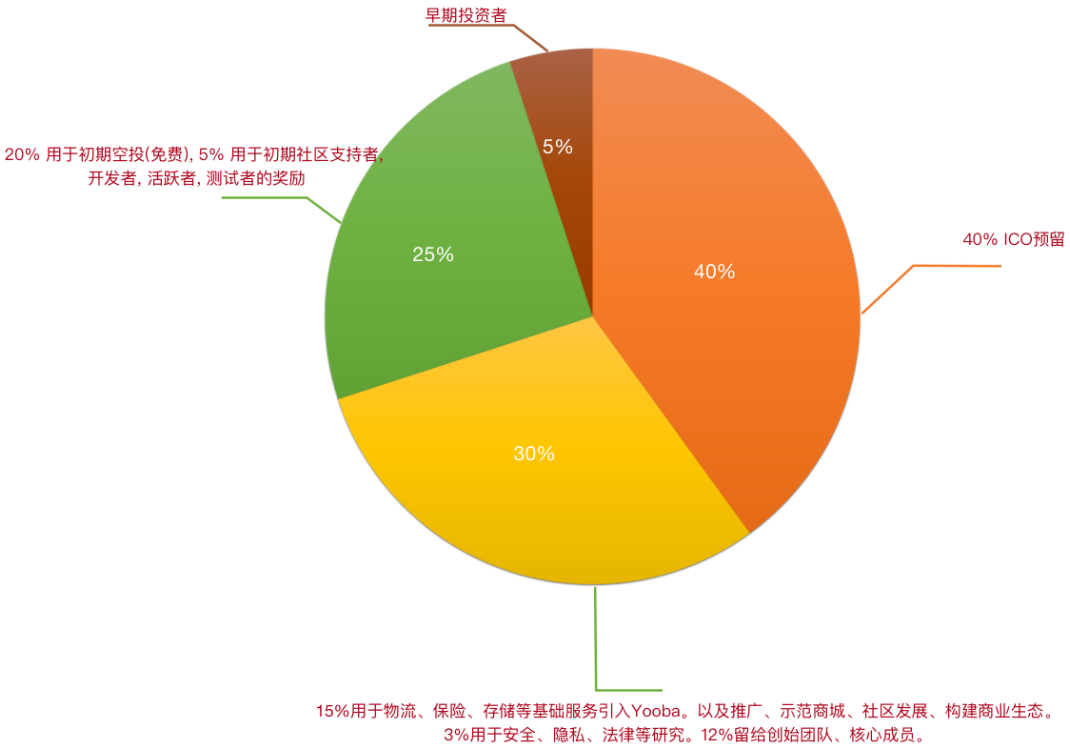
同时我们会制定非常详细的开发计划。便于让每一个有兴趣同时也有能力贡献于 Yooba 的开发者加入到 Yooba 的发展中来。同时这些贡献者也会获得明确的 Yooba token 作为回报。并且越是早期，这些回报数额越大。

我们也会在 Yooba 发展中，不断的吸收优秀的有志加入 Yooba 的贡献者加入到 Yooba 团队中。

Yooba 会成立基金会组织，主要负责 Yooba 的开发、维护、推广、生态发展等。

5 代币发行

代号为 Yoo 的 token 是 Yooba 中用于交易的基本货币。总发行量 100 亿。下图是其发行配比图。



说明：

- 绿色部分 25%早期发放，其中 20%空投，随机免费发放给存有大于 0.01ETH(优先权)的以太坊 Account 地址(感谢以太坊)。空投量 20 亿，大约 20 万地址可以获得 10000 Yoo。会在 2018 年 9 月 30 日前分批次发放完毕，具体发放信息关注官网或 Yooba 社交媒体。另外 5%用于初期对 Yooba 开发、宣传、测试、社区爱好者等的激励。
- 40%用于 ICO 预留。
- 5%提供给早期投资者。
- 30%预留给社区，生态构建，创始团队，科研等。其中 15%留给生态构建和社区。3%留给安全、隐私、法律等研究项目。12%留给创始团队和核心开发者。

通胀率：0.5%~5%

6.代币地位和免责

Yooba 代币 YOO,用作 Yooba 系统内部商品交易媒介和系统运作。

Yooba 代币 YOO 不是 Yooba 主体股票。在 Yooba 主体发展时，您无权获得项目收入的红利。无权分享项目资本或投票权。

Yooba 不保证 Yooba 上交易的安全，不保证 Yooba 上的商品不存在虚假或次品。虽然我们会尽力做好。Yooba 不会承担用户在 Yooba 上交易失败、交易欺诈造成的损失。由于 Yooba 非常高的自由度和隐私性，以及系统的某些不完善，它

存在一定的交易风险，用户需要自行承担其风险。

Yooba 不承担其上销售和存储的产品、服务是否符合当地或国际法律规范的责任、执行人也不承担该责任。由于它是去中心化的和全球化的，我们不能保证其上的每个商品都符合每个地区性的法律。Yooba 是一个全球性参与维护和管理的系统。我们会尽最大努力保护我们的消费者，我们会尽量建议我们的用户只提供符合区域性法律要求的服务。我们会提供部分功能性组件，便于消费者和服务商过滤商品和服务，但 Yooba 不保证能够做到最好。

7 说明

本白皮书会在有重要增加或变动时进行更新。