FirstArk.io 区块链资产交易平台

白皮书（V1.0.1）

（2020 年 12 月 01 日）

目 录

项目背景

在数据爆炸式增长的今天，区块链资产早已成为投资者们趋之若鹜的投资方向。其中，交易所又是该领域中的最具吸引力的投资机会之一。

从当前竞争环境看，头部交易所的行业地位尚未稳固，竞争强度不高；产品形态单一，缺乏差异化竞争；区块链资产交易仍有较大的增量市场。基于以上环境，新入局者仍然有挑战头部交易所的可能。

从用户来源看，当前交易所的用户来源集中度高，全球化进程缓慢。通过相关的数据研究发现，全球 30 家主流交易所的用户来源存在以下的现状：大部分交易所的用户来源高度集中于几个国家；支持语种数量越多的交易所，其用户来源越广泛，全球化水平越高；用户更倾向于在本土设立（或本国人建立）的交易所进行交易。

根据 CoinMarketCap 的数据统计，目前全球区块链资产单日总交易额约为 1500 亿美元，其中单日交易额超过 100 亿美元的交易所仅有 Binance 和 Huobi Global 两家。

现有中心化交易所弊端

虽然去中心化始终贯穿于区块链技术应用的核心，但随着行业进入爆发期，区块链资产交易流动性大增，用户对交易所的要求越来越高。中心化的交易所存在诸多弊端，难以打造更高需求标准。

在区块链资产交易市场，中心化交易所确实对生态系统的发展有关键性推动作用，但同样存在大量的问题。其主要问题包括如下：

交易所安全问题

区块链资产每日数百亿计的交易量在交易所的服务器上进行，这无疑是诱人的蜜罐。用户资产安全保障一直是交易所长期稳定的最重要环节。

2014 年，当时全球规模最大的比特币交易所 MTGOX 65 万枚比特币被盗，平台无力偿还致使破产。

2016 年，Bitfinex 12 万枚比特币被盗，导致用户直接损失 36%的比特币数字资产。

2018 年 3 月 7 日 23 点前后，黑客操控若干 Binance 用户账户，将加密货币通过币币交易换成 BTC，数量达 1 万个 BTC 以上。黑客使用 API 交易机器人用这些 BTC 大量买入 VIA 币，VIA 的价格直接被拉高了 100 倍以上，然后抛售来控制币价。

2018 年 6 月，两家韩国交易所（Coinrail 和 Bithumb）的热钱包遭遇了攻击，其中 Coinrail 损失了 5300 个比特币（价值接近 4000 万美元），Bithumb 损失了近 3100 万美元。

2019 年 5 月 8 日，Binance 的 BTC 热钱包发生被盗事件，据其官方公告显示，这是一次大规模的系统性攻击，黑客获得了大量用户 API 密钥，谷歌验证 2FA 码以及其他相关信息，在区块高度 575013 处从 Binance 热钱包中盗取了 7000 枚比特币。

安全是对用户最根本的承诺，而数字资产安全也是用户与平台长期共存的基石。

用户面临高风险

潜在的操作问题、市场操纵、硬件故障、等待时间过长，以及其它因为交易量巨大所引发的各种潜在问题。同时，目前中心化交易所大量存在技术架构落后、系统不稳定的问题。这些都让用户无法及时、有效的进行操作，投资时效性差，投资受损，极其严重地影响了用户利益，遏制了市场的良好发展。

缺乏信任与透明

中心化交易所的交易进程和实际成本都不透明，手续费往往还很高，由于高峰期的订单不能得到有效管理，通常高于已经公布的费用以及有更多的延迟。同时，他们还可以进行违法的提前交易。

去中心化发展趋势

在以比特币为代表的区块链技术出现之前，达成交易有效的共识总是需要或多或少地依靠一个中心来完成。如果你想完成支付，那么这条交易必须经过一个清分中心（所有的交易都要受它监测）。

而去“中心化是”区块链的典型特征之一，其使用分布式储存与算力，整个网络节点的权利与义务相同，系统中数据本质为全网节点共同维护，从而区块链不再依靠于中央处理节点，实现数据的分布式存储、记录与更新。而每个区块链都遵循统一规则，该规则基于密码算法而不是信用证书，且数据更新过程都需用户批准，由此奠定区块链不需要中介与信任机构背书。

为什么去中心化很重要？它的好处在哪？去中心化至少有三个优点：

1）可容错

去中心化系统不太可能因为某一个局部的意外故障而停止工作，因为它依赖于许多独立工作的组件，它的容错能力更强。

2）抗攻击性

对去中心化系统进行攻击破坏的成本相比中心化系统更高。从经济效益上来说，这是抢劫一个房子和抢劫一片村庄的差别。

3）抗共谋

去中心化系统的参与者们，很难相互勾结。而传统企业和政府的领导层，往往会为了自身的利益，以损害客户、员工和公众利益的方式，相互勾结。

因此，去中心化及去中心化应用是未来发展的趋势，能有效杜绝中心化系统存在的弊端。

去中心化交易所的优势

中心化交易所提供多样的业务模块，如资产托管，撮合交易，资产清算，资产兑换，账户体系等。用户资产都交由第三方集中式托管，这样大大提高了交易速度。简单来讲，中心化交易所将所有人的资产都集中存放在自己的几个钱包里，交易不过是将左口袋的钱转到了右口袋而已，所以相较传统的去中心化交易（区块链上每笔交易都会入块）会迅速很多。同时，主流中心化交易所拥有庞大的用户量与交易量，在交易深度与流动性上也给用户提供了很高的体验感。

在中心化给交易所带来快速的交易与极大的流动性时，也给交易所带来了最大的问题——安全性问题。中心化交易所承担了太多重要角色，用户的资产管理，系统的风险控制，交易的数据保管等。并且所有资产都存储于少数的几个钱包之中，牵一发而动全身，一旦受到黑客攻击损失之大不言而喻。并且，在这样的模式下中心化交易所的权利非常之大，这也带来了潜在

的透明性与安全性的问题。用户数据不透明，交易数据不透明，交易过程不透明，这些不透明性让交易所有了作恶的空间，而作为用户，则没有能力去了解真相。

而去中心化交易所，所有流程都在区块链上进行，并通过开源智能合约实现。这样一来，用户资金不再存放于少数的钱包中，而是分散于节点之间，消除了交易所作恶的空间。用户对自己的资产也有了绝对的话语权，除非私钥泄露，资产被盗的可能性极低。这也降低了用户对交易平台的信用成本。将资产托管、资产清算、撮合交易等都用智能合约来去中心化实现可信的交易机制极大提高了安全性。

关于 FirstArk.io

FirstArk.io 致力于创建一个自治、高效、透明的区块链资产交易平台，让用户可以放心地进行任何规模的交易，而无需担忧平台的公正和透明性、订单系统的完整性和隐私性、或数据安全保护的可靠性。

同时，FirstArk.io 也有别于传统的中心化交易所（甚至不是传统意义上的公司），它迈出了区块链资产交易平台向社区进化的关键一步，是一个公开透明的，通过股权通证（Ark）实现社区自治的新型去中心化交易平台。

平台介绍

币币交易

在过去的几年里，包括 Ethereum 在内的多个区块链网络上出现了众多去中心化交易所。其中，Uniswap 是 Ethereum 上最受欢迎的去中心化交易所，它允许用户从一个简单的网络页面交换各种基于 Ethereum 的 ERC20 代币。截至 2020 年 10 月，Uniswap 的合约担保额为 21 亿美元，占 DeFi 应用锁定的所有价值的 20%。它的日交易量也达到了 2.63 亿美元，约占所有 DEX 交易的 95%。

FirstArk.io 的币币交易模块是基于 Uniswap 构建的一个扩展产品，任何基于 Ethereum 的 ERC20 代币都可以进行交易。用户也可以将任意两个 ERC20 代币组合成一个交易对（不需要

使用 ETH）押注在流动性池中（为流动资金池提供资金赚取收益），由流动性池决定哪些代币上市。

去中心化币币交易的优势？

1）用户的资金不用托管给第三方

与传统的中心化交易所（CEX）不同，我们并不持有用户资金。相反，资金完全由智能合约控制，每次交易完成后，资金会立即存入用户的钱包，没有中心机构可以扣押用户资金。这也意味着用户不需要提供身份信息（KYC）或创建账户。

2）没有中心化的订单簿

币币交易模块不使用订单簿来确定价格，基于“恒定乘积公式”的自动流动性协议。币币交易模块还使用了平均价格数据的预言机。这种方法旨在产生更可靠的价格并防止价格操纵。

3）任何人都可以提供流动性

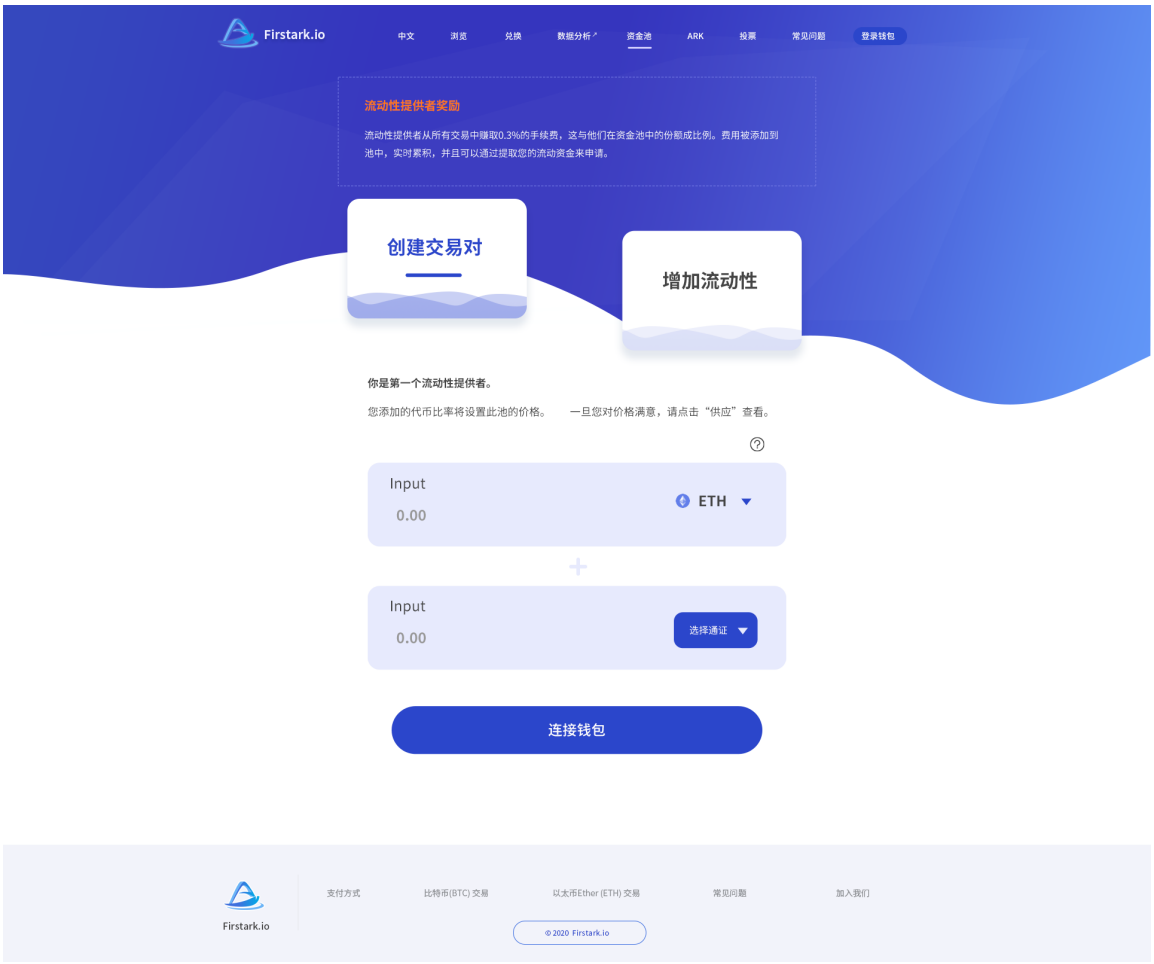
投资者可以通过在流动性池中押注他们的代币来赚取收益。项目方也可以为流动性池提供资金，以促进交易。

币币交易界面预览

币币交易直接链接用户的个人钱包，不使用订单簿来确定价格，基于“恒定乘积公式”

的自动流动性协议。

用户的闪兑操作（买或者卖）会直接影响流动池内的币种数量比，而数量的具体变化则依据恒定乘积公式：X * Y = K（如：X 与 Y 分别代表 USDT 与 ETH 在流动池内的数量，K 的数值在交易中始终保持恒定）。



任何人都可以为某个交易对提供流动性资金支持来赚取收益。

OTC 交易

虽然加密数字资产成功地让人们能够以不可信的方式进行对等交易，但进入或退出加密数字资产交易确没有这样的解决方案。由于中心化交易所固有的不安全属性，数十亿美元的加密数字资产甚至被最受欢迎的服务机构窃取、丢失和摧毁。

以太坊（Ethereum）的推出引入了可编程数字资产，这意味着现在可以通过以太坊的智能合约实现那些中心化交易所无法实现的许多想法。基于信任网和托管系统的想法，我们创建了

一个对等 OTC 交易平台，让用户随时控制他们的加密数字资产。

去中心 OTC 交易的优势？

OTC 交易流程基本与现有中心化交易所一致，但与中心化交易所不同，FirstArk.io 不作为一个中心化的中介机构并吸收用户资金存入，这意味着用户对交易拥有更高的控制权。

1）担保合约

通过以太坊的智能合约技术建立的无信任（Trustless）OTC 交易平台，卖方可以直接将资金存入 OTC 交易平台的担保合约（毋需将 ETH 或 ERC20 的代币转移给任何第三方），除交易双方的人员外，任何他人均无法直接取得对这些 ETH 或 ERC20 的代币的控制权，我们只能在其中一方发起申诉的情况介入并干预交易的进行。

2）地理位置

你可以搜索指定国家或城市的订单，或将搜索范围设定为全世界（如果你对交易对方的所属地区不敏感的话）。

3）支付方式

有多种可选的支付方式，包括：银行转账、支付宝、微信、PayPal、现金交易（面对面）以及国际汇款等等。根据你选择的地理位置，支持的交易方式可能会有所差异。

4）交易币种的延迟释放

卖家可以设置交易币种的延迟释放，这意味着买家只能在交易成功 24 小时后才能取得资金。当然，这种设置可能会影响你的成交几率（买家更愿意交易结束即获得交易币种）。

5）争议的解决

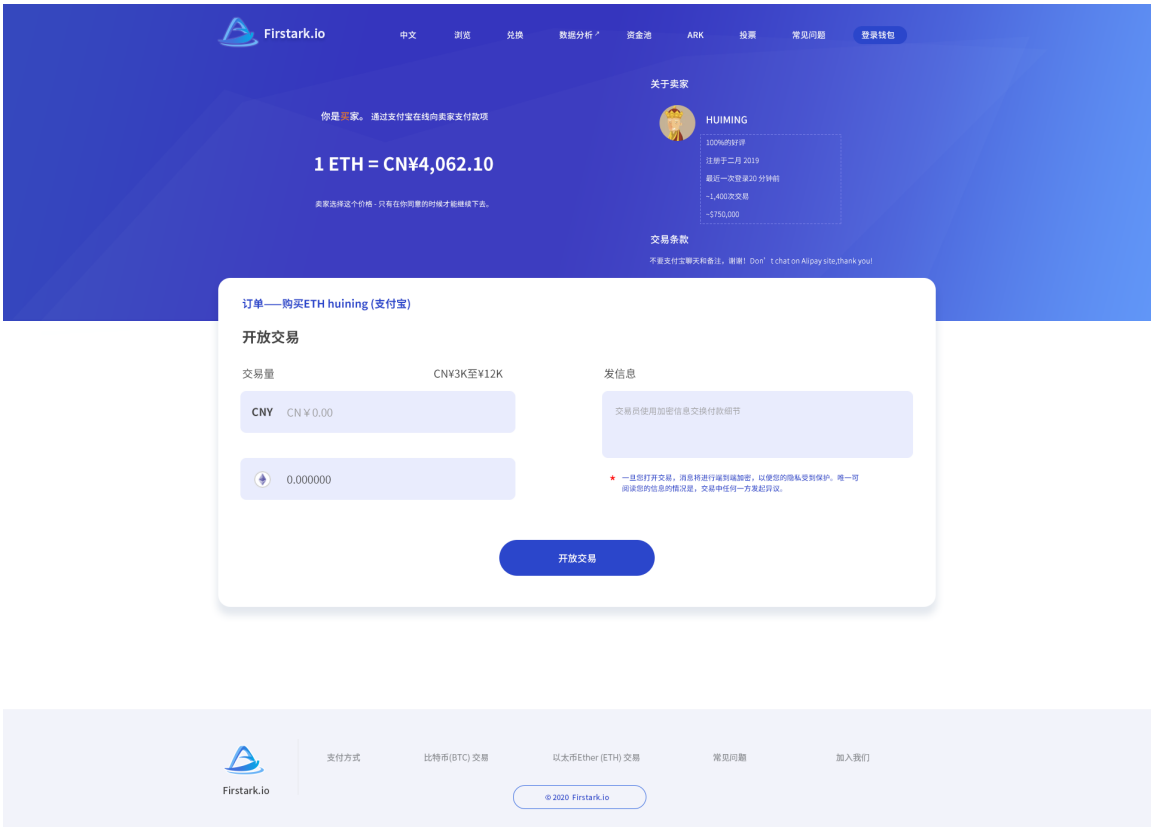
任何一方都可以提出争议，要求第三方仲裁员（现为 FirstArk.io 的工作人员和部分由社区竞选出的仲裁节点）作出解决。

仲裁员可以要求提供证据（例如买方的付款证明），以帮助确定哪一方是资产的合法所有人。 根据争议的复杂程度，他们可能需要几分钟、几小时、几天甚至几周才能做出决定。

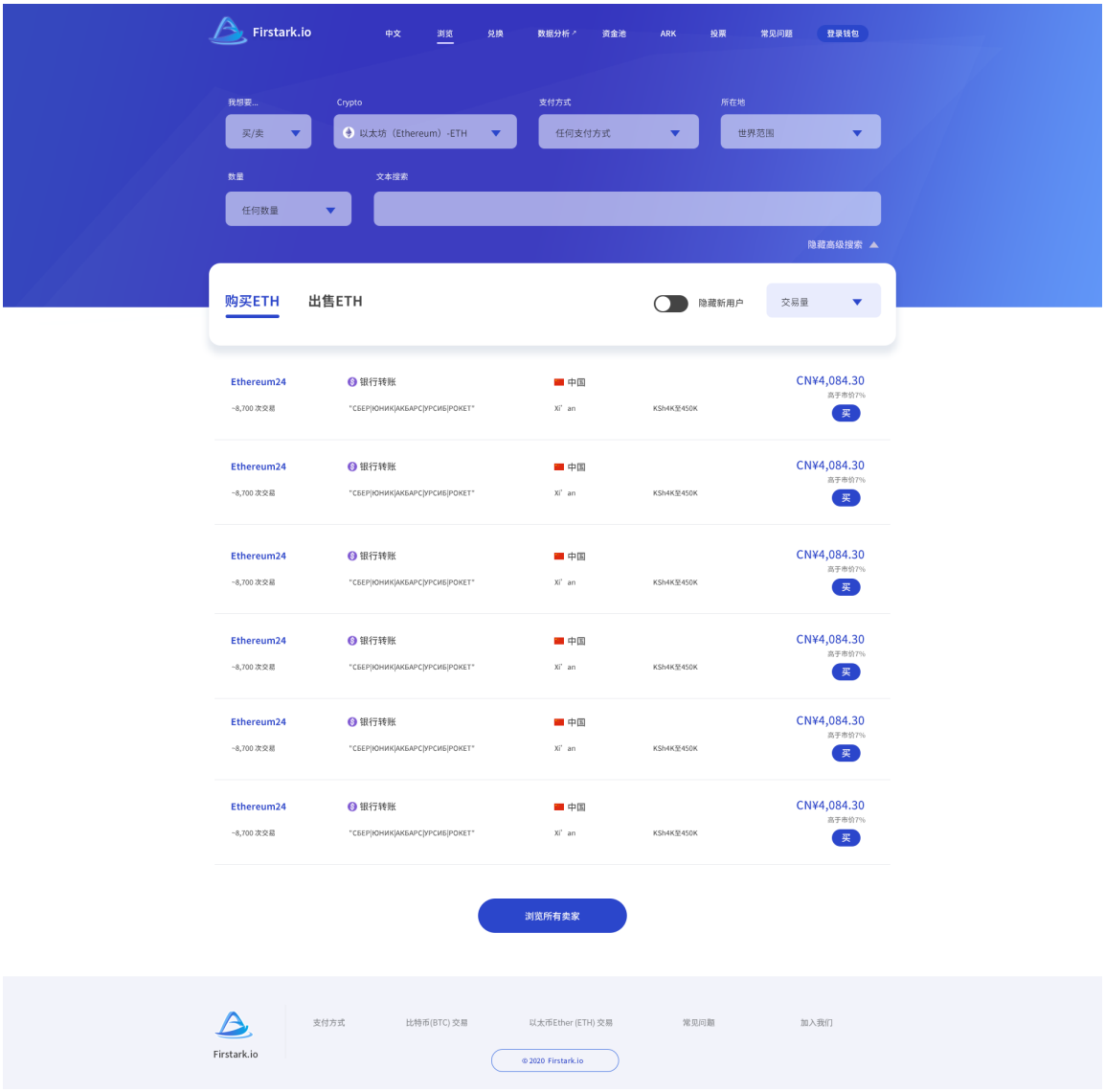
一旦仲裁员有足够的证据确定资产的合法所有人，他们便可以将代管合约中的资产释放给其中一方（**智能合约代码不允许他们将资产发送到其他任何地方**）。

OTC 交易界面预览

用户直接通过个人钱包登录，FirstArk.io 并不作为一个中心化的中介机构并吸收用户资金存入。



操作界面与传统的中心化交易所差别不大，方便用户快速上手操作。



支持多币种、多地区，以及多种可选的支付方式，包括：银行转账、支付宝、微信、PayPal、现金交易（面对面）以及国际汇款等等。

代币存管服务

默认情况下，您的以太坊（Ethereum）交易记录和余额都是公开的。所有交易都可以在 Etherscan 等区块浏览器上看到，任何知道您以太坊地址的人都可以轻松查看您的交易记录，追踪资金来源，计算持有量并分析您的链上活动。

但是，如果您不希望所有人公开查看您的交易记录和余额，该怎么办？如果在交易时需要匿名和隐私怎么办？

代币存管服务如何在以太坊中实现隐私交易？

代币存管服务通过断开接收地址和发送地址之间的链上链接来提高交易隐私性。使用可以接受不同以太坊地址提取 ETH 或 ERC20 代币存款的智能合约，每当以新地址提取 ETH 或 ERC20 代币时，都无法将提取的资金与存款者相关联，从而确保完全的隐私。

1）存款

用户生成一个凭证并将其哈希值连同存款金额一起发送到代币存管服务的智能合约，合约接受存款并将凭证添加到存款清单中。

之后，用户提款应提供智能合约存款清单中未使用过的凭证。智能合约将检查凭证，并将存入的资金转移到指定的提款地址。外部观察员将无法确定此提款来自哪个存款。

2）提款

提款有两种选择，使用钱包（Metamask，TrustWallet 等）或通过中继器发送。

钱包提款要求您拥有一个全新的以太坊地址，上面带有一些 ETH（用于支付以太坊交易的 Gas 费用）。这又是一个问题，如何在提款地址上获取一些 ETH 而又不会失去匿名性？

通常您是从其他人那里购买（或使用交易所），而我们刚好就是想避免这种操作，对吧？

因此，您可以使用中继器功能来完成此过程。您所需要做的就是生成一个新的以太坊地址，然后 zkSnark 证明和中继器合约将会完成其余工作。它还会向您收取一些 ETH，以支付以太坊交易的 Gas 费用。

3）保持匿名的提示

无论是否使用中继器，您仍然需要保持常用的 Internet 匿名性，例如使用 VPN、代理或 Tor 来隐藏您要使用的 IP 地址。

等到有几笔存款之后。如果您的充值和提款是紧挨着的，那么观察者可以猜测这可能是同一个人。我们建议您等待至少 5 次存款。

等到存入资金一段时间之后。即使您之后有多个存款，它们也可能都是由同一个人进行的，这些人都试图发送垃圾存款，并使用户错误地认为存在大量匿名性。我们建议至少等待 24 小时，以确保在此期间多人进行了存款。

多语言支持

作为全球性国际化交易平台，我们在产品和技术设计时，我们就做好了多语种的准备，在设计实现时，将语言资源文件做成可配置的版本，保证了快速扩展与扩容。

我们在上线初始将支持英文和中文，在半年之内，再完成对日语、韩语、俄语和阿拉伯语等语言支持。

代币发行细则

ARK 代币

FirstArk.io 推行的代币为 ARK，是基于 Ethereum 区块链的 ERC20 标准代币，发行总量恒定为 2 亿枚，且保证永不增发。其中 10%为基金会保留（用于平台运营、商业推广、社区激励等生态发展上），10%用于创始团队保留，10%用于募集平台建设资金，剩余的 70%给 FirstArk.io 社区成员（用于流动性挖矿产出等）。

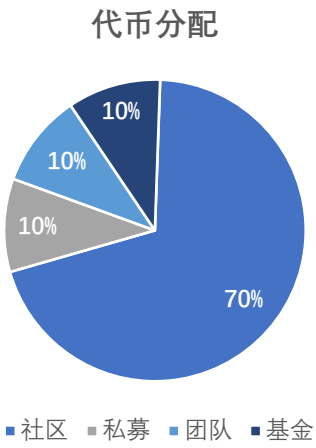
ARK 分配如下：

1、10%基金会保留（20,000,000 ARK）；

2、10%创始团队保留（20,000,000 ARK）；

3、10%投资者募集（20,000,000 ARK）；

4、70%给 FirstArk.io 社区成员（140,000,000 ARK）。



每个部分的代币均分 4 年逐渐释放，第一年释放 40%，第二年释放 30%，第三年释放 20%，

最后一年释放剩下的 10%。

资金分配

公开发行所筹资金，按以下比例进行分配：

30% 用于平台的技术开发（包括员工激励、项目研发经费、智能合约审计等）；

50% 用于平台的市场拓展（包括品牌建设和运营推广，为市场活动提供资金支持，以推进平台在世界范围内的用户接受度，从而快速积累用户）；

20% 作为平台的储备基金，以应对各种突发状况。

代币价值

1）利润分红

平台所有可能产生的收益均进入分红合约，ARK 的持有者可以将其持有的 ARK 锁仓到分红合约，按其锁仓比例提取某个分配周期内的平台收益（例如：在某个分配周期内，ARK 持有者 A 锁仓的 ARK 占分红合约中 ARK 总量的 5%，那么 A 就可以通过分红合约提取该分配周期内 5%的平台收益）。

2）参与决策和管理

每个 ARK 持有者都有权利参与社区的业务决策和管理活动（如：上币投票，OTC 交易的申诉仲裁等），FirstArk.io 是一个所有 ARK 持有者共有、共治、共享的社区型组织。

风险提示

本文仅作为传达信息之用途，文件内容仅供参考，不构成本项目的任何投资买卖建议、邀约或要约。任何与本白皮书相关的行为均不得视为参与公开发行，包括要求获取白皮书的副本或与其他人分享白皮书。参与公开发行则代表参与者已经达到年龄标准，具备完整的民事行为能力，充分了解所有风险。

免责声明

本项目 Token 的增值与否取决于市场定价规律以及项目实施后的需求，极端情况下或因不可抗力因素影响，可能不具备价值，没有正确使用 Token 的人有可能失去使用 Token 的权利，甚至可能会失去他们的 Token。

本项目团队不对其增值做出承诺，并对因价值变动造成的后果不负责任。我们承诺尽一切可能确保您的资产与交易安全。