小蚁(ANS小蚁股)-智能资产及应用平台

概述

- 小蚁是国内最早的开源公有链项目，是一个智能资产平台。智能资产是将区块链的智能合约与数字资产相结合，使得在小蚁上注册、发行、流转的数字资产更加智能化。
- 数字资产是以电子数据的形式存在的资产，用区块链技术实现资产数字化有去中心化、去信任、可追溯、高度透明等特点。小蚁底层支持多种数字资产，用户可在小蚁上方便地自行注册分发资产，自由交易和流转，并且通过数字证书可以解决公有链的信任问题，用户通过数字证书所注册分发的资产也会享受到法律的保护。对于逻辑更加复杂一点的业务场景来说，他们同样可以利用智能合约来强化资产的功能，或者创建一种与资产无关的业务逻辑。
- 智能合约是1994年由密码学家尼克萨博（Nick Szabo）最先提出的理念，几乎与互联网同龄。根据Nick Szabo的定义：当一个预先编好的条件被触发时，智能合约执行相应的合同条款。区块链技术给我们带来了一个去中心化的，不可篡改的，高可靠性的系统，在这种环境下，智能合约才大有用武之地。小蚁有图灵完备的智能合约，在小蚁区块链虚拟机（AVM）中执行并且拥有确定性、可终止性、资源控制、并发、分片与无限扩展等众多优点。

基本信息(数据截止2017/6/15)

- 发行日期：2016-9-9
- 市值排名：41
- 交易量前三大交易平台：云币网 / 元宝网 / 聚币网
- 官网：https://www.antshares.org/zh-CN

- 钱包下载：https://www.antshares.org/Download/Index
- 区块链浏览器：http://antcha.in/

市场关注度(数据截止2017/6/15)

- 推特：未开通
- github：333
- slack：未开通
- 官网全球排名：293860

创立

- 小蚁运营公司CEO达鸿飞：2011年接触比特币，中国比特币社区的早期参与者。2013年起全职从事数字货币社区工作，联合创立了“比特创业营”。多次在北京、香港等地的数字货币峰会担任演讲嘉宾，担任多个区块链创业项目的顾问。2015年起开始主持“小蚁”项目，用区块链技术让普通公司都可以进行“数字IPO”，发行股权，交易股权。

核心团队（部分）

- 张铮文（CTO）：小蚁核心开发者区块链技术和计算机安全专家，CISA信息系统审计师。中国屈指可数的具备区块链底层协议架构和开发能力的技术专家，dBFT共识机制的作者，独立原创实现了小蚁全部的核心代码。曾任职于盛大游戏、火币网等公司，从事信息安全和数字货币研发等工作。

- 林鹏涛：小蚁开发者之一，2013年接触比特币，2014年开始在火币从事比特币相关开发，熟悉web与区块链开发技术，目前正在参与小蚁钱包的设计与开发工作。

项目进展

- 官网改版：小蚁官网已于5月12日进行了改版，除了视觉方面的优化，在内容方面新版本主要增加了技术文档，可以通过技术文档来了解小蚁和进行私有链搭建、智能合约编写的学习。

- 团队壮大：在5月最后两周，迎来了两位负责市场运营的人才，分别是之前在七牛负责开发者关系维护的Sharlyne和具有近8年投资经验、热衷区块链技术的陈衢，将共同筹备6月22日智能合约2.0与品牌战略发布会。

- 开发大赛闭幕：5月25日，由上海市科委指导，INNOSPACE创客空间联合小蚁区块链举办的“区块链开发比赛”圆满落幕。此次比赛的视频直播在线观看人数达到5000人次。

- 蓝鲸淘上线交易：5月15日，小蚁生态中的智能资产管理平台蓝鲸淘平台上线了开拍币/小蚁股交易，作为去中心化交易平台，蓝鲸淘将资产的控制权掌握在用户手中，大大降低传统的平台跑路风险和黑客攻击风险。需要注意的是，交易的价格不是以CNY为单位，而是以交易规定的代币为单位。

- 生态资讯：5月19日，小蚁区块链核心开发者张铮文参加了“2017云计算技术大会”，在会上演讲了“电子现金——智能合约——智能资产”的区块链演进之路。
- 5月26日下午，2017贵阳数博会“区块链高峰对话”上，小蚁创始人、Onchain（分布科技）CEO达鸿飞分享了“从跨链到跨生态”的区块链进化论体系——跨链互操作协议和全新的智能合约技术，正在助力区块链实现质的飞跃。

发展路线图

- 2014.6 小蚁正式立项，接受种子轮投资。
- 2014.8 正式组建小蚁团队和小蚁运营公司
- 2014.6 小蚁前端生态“微天使”上线
- 2015.6 在GitHub上建立antshares项目，并实时开源
- 2015.9 小蚁团队正式发布小蚁区块链白皮书
- 2015.10 小蚁ICO一期众筹2100BTC
- 2015.11 小蚁测试网上线，发布测试版节点客户端
- 2016.4 小蚁发布国内第一个原创共识机制dBFT
- 2016.5 陶荣祺等一大批优秀的人才加入小蚁团队
- 2016.6 小蚁团队赞助2016区块链国际峰会
- 2016.7 Onchain申请antshares成为超级账本第三个子项目
- 2016.8 小蚁ICO二期全球开启，众筹6119BTC
- 2016.8 第一个由小蚁爱好者组建的小蚁社区 antfans.org 上线
- 2016.9 毕马威首次发布中国金融科技创新50强榜单，小蚁区块链与财付通、京东金融、陆金所、蚂蚁金服、微众银行共列榜单。
- 2016.10 小蚁区块链，主网正式启动上线。
- 2016.10 小蚁首个社区开发的区块链浏览器antcha.in上线
- 2016.10 小蚁正式上线云币、元宝网、19800、Bittrex等交易所
- 2016.10 2016年度优秀区块链平台10强榜单小蚁再次入榜
- 2016.10 小蚁与Wings达成全方位战略合作，将共同开发市场和区块链技术
- 2016.11 小蚁团队发布Antshares VM轻量级通用型区块链虚拟机白皮书
- 2016.12 小蚁区块链将与萌果VR团队合作，探索游戏+区块链技术
- 2017.2 小蚁生态首家将超导交易2.0落地的交易流转平台“蓝鲸淘”开始公测
- 2017.2 小蚁生态迎来新区块浏览器antchain.xyz
- 2017.2 基于小蚁区块链的智能基金Nest上线官网nestfund.io 收起

早期投资人

- 镭厉资本

分配与发行

- 众筹时间：第一次众筹：2015年10月，第二次众筹：2016年8月
- 总量：1亿
- ICO发行量：5000万

- 约10%的小蚁股在2014年6月被分配给了小蚁的早期支持者，获得了60万元的种子资金。其中40万元由若干个人按500万整体估值出资，20万元由风险投资机构镭厉资本按1000万元整体估值出资。个人出资者同时还无偿地全职或兼职地提供了各种支持。

- 约17%的小蚁股在2015年10月完成的ICO 1分配给了参与者，获得了2100个比特币。其中约1200个比特币来自个人投资者，约900个比特币来自一个机构投资者。

- 约23%的小蚁股在2016年8月启动的ICO 2中分配给参与者。本次ICO不设价格和上限，但设计了可退回机制。

- 剩余的50%的小蚁股由小蚁团队持有，将在小蚁主网上线后利用小蚁智能合约锁定1年。1年锁定期后，这部分小蚁股将用于维护小蚁的长期发展运营。

项目分析

- 设计目标：小蚁的愿景（mission）是“每个人的数字资产”。小蚁希望构建一种能够对接实体世界资产的桥梁式的金融系统。小蚁面向的用户群体是广泛的互联网主流用户，而不仅仅是自由主义者、极客和开发人员。为了实现这一愿景，小蚁需要在底层上采用不同的设计。

- 用电子合同取代代币：区块链领域进行资产数字化的通行做法是“代币化”（tokenization）。即用户发行一种自定义代币，并声明该种代币代表了某种资产。随后这种代币就可以像比特币一样在用户间进行流转、交易。然而代币化在法律上有诸多瑕疵。代币的流转类似于转账——无需接收方同意，代币就能从发送方流转到接收方手中。这种流转只适合用于货币这样的仅有权利而无义务的资产，而不适用于股权、债权等具有复杂的权利义务的资产。因此，小蚁中资产的流转以电子合同的形式完成，大部分的资产转让需要出让方和受让方各自以私钥进行电子签名。在某些情况下，还需要资产发行人参与签名。在小蚁区块链上以电子合同的形式记录资产流转，仅仅是线下资产流转的一种新型链上解决方案，不创设新的法律关系，解决了代币化的法律瑕疵。

- 用户控制的身份认证：

    - 实名身份信息是大量实体世界资产的确权基础。大多数情况下的法律合同（legally binding contract）也要求实名签署。当交易所在地法律或交易参与方有实名的需求时，用户应该有证明其真实身份的能力。同时，这种身份信息的公开范围应该受用户控制。该笔交易外的第三方不应该获得用户身份信息。同时身份认证仅仅是一种可选项，而非强制。当交易参与方都不要求对方实名时，用户无需做身份认证。

    - 小蚁使用数字证书来实现用户身份认证。用户（个人或机构）都可以向数字证书认证机构（CA - certificate authority）申请数字证书，以证明其所控制的公钥和其身份之间的对应关系。小蚁并不指定CA，而是由交易参与方自行选择自己认可的CA。例如中国的用户在进行股权转让时既可以选择工信部认证的38家CA机构中的任意一家，也可以选择由登记该股权的公司担任CA，查验身份颁

发证书。

    - 与X.509数字证书实现方案不同，小蚁计划使用区块链来维护证书撤销列表（certificate revocation list），并逐步形成一套基于区块链技术的数字证书体系和身份认证方案。

- 无分叉的确定性记账：区块链现有的共识机制可以被分为两大类：“单人记账”和“联合记账”。

    - 比特币、以太坊、比特股等区块链均使用单人记账模式。单人记账模式下，单个节点符合一定规则（如所持算力、权益、选票）即可完成单个区块的记账工作。其他节点通过在此区块后追加新的区块，表达对该区块的认可。追加区块就像在对历史进行投票。当发生分叉时，哪个历史的票数更多（链更长），这个历史就是大家的共识。

    - 单人记账下的交易确认是一种概率的表达，例如：获得一个确认（交易被包含进一个区块）的交易成为历史共识的可能性是98%，获得两个确认（包含该笔交易的区块后面被追加一个区块）的交易成为历史共识的可能性是99%，而六个确认的则可能是99.999999%。但理论上，即便是一万个确认也仍然存在被推翻的极微小可能。比特币等区块链通过添加人工检查点，写死了较久远的历史，避免此类极端情况。

    - 如果说单人记账模式通过事后投票（追加区块）的方式来进行共识，联合记账模式则通过事先决议的方式来产生确定性的记账节点，从而避免了事后投票，获得了确定性。在公有链中，这种事先决议可以是链上投票选举。选出一批记账节点后。每个新的区块均由这些记账节点共同签名确认。这样就把“事后投票，确认越多概率越高”的模型改变成了“事先投票，确认即最终”的模型，获得了理想的交易最终性（finality）。

    - 单人记账里的事后投票（追加区块）是对区块内容而非对区块生成者的投票，因此适合无身份信息的公有链。但单人记账模式下，交易的最终性较弱，不太适合金融交易。联合记账模式需要引入对记账节点的弱信任，即相信不会有大量（一般指1/3或以上）的记账节点勾结作恶。那么这就需要对这些记账节点的控制人的身份有所了解，一来可以判断其声誉和技术能力，二来如果作恶，可以用密码学证据进行事后举证追责。因此联合记账适合有身份信息的公有链和联盟/私有链。

    - 一般认为单人记账模式有较好的可用性，即在发生网络分区时（如一国与他国的互联网线路完全断开）仍然能够较好的工作。但这种可用性只适用于跟随了较长链的节点。当网络分区恢复时，跟随较短链的节点所看到的历史会被长链所改写。对于跟随较短链的节点而言，这是一种牺牲一致性换得的虚幻的可用性。

    - 可以说单人记账模式选择了匿名性，实现了无需对任何节点的信任，但牺牲了一致性、最终性；联合记账模式选择了一致性、最终性，但需要记账节点提供身份，以获得其他节点对其的弱信任。

    - 记账节点是小蚁区块链的最核心角色，受小蚁股持有人的委托负责参与共识，制造区块；全节点是小蚁区块链网络的主要组成部分，一般由提供对外服务的服务提供商运行，保存完整的历史数据，侦听并转播交易；而普通用户则运行轻节点或仅仅作为客户端接入。普通用户通过浏览器或移动App接入小蚁生态上的服务提供商，只同步和保存自己有关的数据。由于小蚁区块链使用了基于弱信任的联合记账模式，区块中包含了记账节点的数字签名，普通用户无需下载完整历史数据也能对当前区块进行校验。

- 低延迟、高吞吐、可插拔：
    - 可扩展性是制约区块链技术和传统技术竞争的一大因素。比特币为了实现抗审核和无需信任的设计目标，选择了工作量证明这一共识机制，同时也带来了高延迟、低吞吐的性能问题。小蚁使用了依赖弱信任的共识机制，并专业化了记账节点，做到了低延迟，高吞吐。小蚁的共识机制保证了确定性的小范围的专业性的记账节点名单，从而实现了低延迟和高吞吐。
    - 目前小蚁的出块时间被人工限定为15秒。未来当记账节点之间的网络连延迟足够低时，大部分区块有望在1秒内完成。在100Mbit/s的带宽下，通过外置硬件实现密码学计算，小蚁区块链每秒可以处理数千到万级的交易量。
    - 另外，小蚁采用可插拔模块化设计。用户可以自换共识机制，ECC/散列算法，P2P网络协议等模块。同时，只要把小蚁股视为联盟/企业的投票权，小蚁就可以很容易的改造为联盟/私有链。商业机构可以在小蚁公有链上进行概念验证，如有需要则可以快速迁移到联盟/私有链模式；反之，商业机构先运营小蚁派生的联盟/私有链，如有需要则可以快速迁移到小蚁公有链，而无需对周边系统大动干戈。
- 分层设计和超导交易：
    - 为了在支持多种资产，多类型交易的同时达到良好的扩展性，分层设计是必不可少的。Ripple、比特股、NXT等带有去中心化交易所功能的区块链没有采用分层设计，由区块链本身实现订单簿和交易撮合功能。在这类区块链上，挂单、撤单、撮合等操作均记录在区块链上，这种设计具有多重弊端。小蚁区块链只负责交易的执行和结算。分层设计中把订单簿和撮合功能放在第二层，通过一种叫做“超导交易”的机制来实现完整的交易功能。
    - 超导交易下交易双方不需要把财物托管给一个中介（传统交易所）。用户仅仅需要把用私钥签名过的订单发送给交易所，交易所完成买方和卖方的订单撮合后，在小蚁区块链上广播交易，完成结算。自始至终财物不离开用户的控制，杜绝了传统交易所的道德风险。超导交易机制下的交易所仅仅起到信息撮合的作用。
    - 在超导交易机制下，由于用户拥有绝对的控制权，因此用户可以通过主动双花导致订单无法被结算。这一问题可以通过交易所将该用户列入黑名单予以惩罚和震慑来解决。

最新动态

- 小蚁将于2017年6月22日在北京举办 NEW小蚁品牌战略发布会，并将以「智能经济」为主题，与区块链圈内专家、技术人员、媒体及VC共同探讨与交流。
- 2017年6月16日直播“关于5千万限制流通小蚁股使用分配情况说明”。