小蚁白皮书 1.1

该文档正在编辑中，我们会尽快完成，你可以在 Github wiki 上查看其它文档，或者来我们的 小蚁官方网站 逛逛。

小蚁是一个开源的社区项目，如果你感兴趣，你也可以通过 pull request 的方式来贡献开发文档，开发文档的项目地址为 github.com/AntShares/docs ，感谢您的付出。

小蚁概述

小蚁与区块链

什么是小蚁

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。

小蚁区块链通过将点对点网络、拜占庭容错、数字证书、智能合约、超导交易、跨链互操作协议等一系列技术相结合，让你快速、高效、安全、合法地管理你的智能资产。

什么是区块链

区块链（blockchain）一词来源于比特币。中本聪在比特币白皮书中提到了“chain of blocks”，随后在其发布的第一版比特币程序中，把保存交易数据的文件夹命名为了blockchain。最初blockchain仅指比特币的历史交易数据。随着各种加密数字货币（crypto-currency）纷纷采用blockchain命名其交易数据文件夹，blockchain逐渐被用来指代各种加密数字货币的历史交易数据。

从2015年开始，国际主流金融机构开始陆续研究比特币、以太坊、Ripple等类似的系统。这些金融机构把比特币等类似系统的底层技术和上层业务做了分离，并用blockchain technology来指代这套底层技术组合。区块链技术不是单项的技术创新，而是对数种已有技术的创新技术组合。一般来说，区块链技术使用到了密码学、网络拓扑学、一致性算法、博弈论等基础学科的知识，并在这些基础学科知识上实现了工作量证明、权益证明、智能合约、闪电网络、侧链等技术模块。

区块链的技术核心

我们认为，区块链的技术核心是**如何达成分布式共识**——即在没有中心或具有多个中心的网络中，各个节点如何对该网络内所发生的所有事务（transactions）达成一致认识。这些一致认识包括了事务的内容、有效性、时间顺序等要素。

- **通过数字签名对事务内容、有效性达成分布式共识**

  在传统的纸质系统内，事务内容（交易指令）往往和鉴权信息（签字盖章）分别存放。比如银行窗口取款时，用户签字确认的申请单和银行系统的交易记录账本是分开存放的。这样一来，就无法银行以外的人员就难以对这些交易指令的真实性进行验证。

  区块链系统将事务内容和鉴权信息绑定存放（bundling）。各个节点无需借助中心机构，仅凭数字签名就能自行验证交易指令的完整性（未经篡改）和有效性（签名者有权限），从而实现了对事务内容和有效性的分布式共识。

- **通过共识机制对事务顺序达成分布式共识**

由于点对点网络下存在较高的网络延迟，各个节点所观察到的事务先后顺序可能不一致。因此区块链系统需要设计一种机制对在一定时间内发生的事务的先后顺序进行共识。这种对一个时间窗口内的事务的先后顺序达成共识的算法被称为“共识机制”。常见的共识机制包括：

- 工作量证明：比特币、以太坊（现在）
- 权益证明：点点币、NXT、以太坊（未来）
- 代理权益证明：比特股、Crypti、Lisk
- UNL/Quorum Slice：Ripple、Stellar
- 拜占庭容错共识：小蚁、Hyperledger Fabric

- **通过散列算法对历史数据达成分布式共识**

  区块链系统一般会通过引用前一区块的散列值（哈希）的方式，构造一种链式结构，实现类似于“骑缝章”的效果。任何对单笔交易内容进行的篡改都会引发绑定的数字签名的失效；任何对交易顺序进行的篡改，又会引发区块散列值的变化，导致“骑缝章”无法对上。因此，任何节点都可以无需借助于中心机构，自行验证全部的历史交易的有效性，对此达成一致认识。

- **通过“智能合约”对计算结果达成分布式共识**

  Nick Szabo在1993年提出了Smart Contract的概念，远早于区块链的出现。比特币的脚本系统是对智能合约概念的第一个基本实现。以太坊在其基础上做了较大的发展，实现了一个更为灵活的图灵完备的智能合约平台。此外，Hyperledger也实现了基于容器技术的智能合约（其称之为chaincode）。

  我们认为区块链之上的智能合约是在对事务的内容、有效性、顺序、历史数据等达成共识的基础上，以这些数据作为输入，对计算得出的结果所达成的再一次的分布式共识。

除了以上的各种共识的达成，区块链技术还包括了闪电网络、侧链、跨链交易、隐匿地址（Stealth Address）、保密交易（Confidential Transaction）等不仅仅局限于分布式共识的技术模块。

设计目标

小蚁的愿景（mission）是“每个人的数字资产”。比特币等区块链希望构建一种平行于实体世界的平行金融系统，而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。同时，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。

合规对接实体世界

- **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。

满足金融交易需求

- **无分叉的确定性记账**

我们认为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。

- **使用法币作为货币**

货币的核心职能有三：交换媒介、记账单位和价值存储。比特币等加密数字货币是良好的交换媒介，用户可以通过比特币作为媒介在全球转移财产。然而加密数字资产普遍的非弹性带来了高波动性，从而无法实现记账单位和价值存储的完整货币职能。比特股、Nubits等系统试图设计一种可以锚定法币的稳定加密数字货币，然而并不十分成功，应用范围狭窄。

小蚁使用法币作为内部货币。

- **节点的分工与专业化**

中本聪最初对于比特币的设计目标是极为扁平化的。所有的节点都参与：记账（挖矿）、存储完整历史数据、转播交易，没有专业分工。然而在实践中比特币逐渐演化出了专业分工。记账（挖矿）已经从中本聪设想的“one CPU one vote”一路演进出了使用GPU、FPGA（现成可编程逻辑门阵列）和ASIC（专用集成电路）的矿机。目前ASIC矿机以外的计算设备已经不可能经济地进行挖矿。记账节点已经完全专业化。

比特币过去7年的几十GB的历史数据也成为了一种存储负担。许多普通用户不再愿意运行需要存储完整历史数据的全节点，而是转而使用web钱包、off-chain钱包等等。尽管有呼吁运行全节点的各种呼声，然而全节点的数量却在持续下降中。

在小蚁里我们的设计目标是让整个系统有清晰的角色分工。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。我们认为这样的模式有利于实现“每个人的数字资产”这一小蚁的愿景。

需要说明的是，上述弱信任不是对某个记账节点的信任，而是对记账节点这一团体不会勾结作恶的弱信任；不是被动的中心化机构指定的信任，而是以去中心化的方式由用户自主投票选择的弱信任。

高扩展性的架构设计

- **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：

- 挂单、撤单需要等待区块确认，延迟高体验差
- 挂单、撤单需要支付交易手续费，还增加了存储和带宽消耗
- 由于存在买卖交易，交易的顺序变得极为重要。将订单簿和交易撮合在区块链层实现，就赋予了记账节点更大的特权，记账节点能够按照其意愿对交易进行排序、取舍，拥有了抢先交易（front-running）的能力。

尽管小蚁支持链上的资产互换交易，但是小蚁区块链本身并不提供订单簿(order book)和撮合(order marching)功能。小蚁区块链只负责交易的执行和结算。我们的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。

应用场景

股权众筹和股权交易

小蚁可以被用于股权众筹。发起股权众筹的公司仍然通过各个众筹平台完成募资，但过程中可以利用小蚁区块链的不可篡改特性，将募资的公开文件用小蚁区块链来存证。众筹完成后，公司可以用小蚁来进行股权的登记，向众多的投资人发放股权份额，避免了繁琐的纸质文书和线下人工。小蚁区块链上的股权份额是一种可以具备一定流动性的资产，用户可以通过小蚁进行点对点的股权交易。合规的交易场所也可以对接小蚁，提供非上市公司的股权交易服务。通过小蚁，初创公司获得了市场估值、股权流动性，用户获得了退出机制，解决了股权众筹退出难的痛点。

另外，小蚁还可以便于进行众筹额度管理。近年来，各国都在出台有关股权众筹的法律法规。这些法律法规中往往会对投资人的合格性、投资额度等做出具体规定。例如2016年4月生效的美国JOBS法案第三部分（JOBS Act Title III）就规定单个投资人最高每年投资股权众筹的总额不得超过10万美元。通过小蚁可以便于监管层对这一总额进行有限管控。

员工持股计划和资本结构表管理

采用员工持股计划（ESOP）和需要进行资本结构表管理（cap table mangement）的公司可以用小蚁来进行股权管理。美国的一些公司已经采购了类似eShares这样的中心化的服务商来进行资本结构表（cap table）的电子化管理，然而中心化的系统具有诸多弊端。例如eShares就是一个单一故障点（single point of failure）,一旦eShares服务宕机、倒闭、被黑，那么使用eShares服务的公司的股权信息数据就危在旦夕。

基于区块链技术的小蚁比此类中心化系统更经济更安全。没有单一故障点，因此使用的公司无后顾之忧。小蚁的智能合约功能还给了公司灵活的股权转让控制权。公司可以限制股权仅可以被指定的员工和投资者持有，可以灵活的设置允许股权转让或交易的比例。比如可以设置为允许员工每年最多转让其本人所持股权的10%。

目前，提供ESOP解决方案的咨询公司的解决方案仍然通过纸质文书来完成。通过小蚁，这类咨询公司可以向客户公司提供数字化管理股权的强大工具。

P2P借贷

P2P借贷平台使用小蚁区块链可以解决信息不透明，征信不全面，债权不易再流转等多个现存问题。

首先，现有模式下P2P借贷平台的内部数据库是唯一的债权确权依据，一旦发生黑客篡改、数据灭损、平台倒闭等事件，债权人难以证明自己的债权份额。在2015-2016的中国P2P借贷平台的倒闭潮中，这一风险已经暴露。一些P2P借贷平台"跑路"后，在这些平台上实行分散投资降低风险的债权人发现，P2P借贷平台的网站已经不可访问，自己陷入了无法证明自己所持债权的境地。

其次，P2P借贷平台对借款人的信用额度控制往往仅局限于平台自身。例如某平台通过征信程序认为借款人的还款能力为10万元，那么在此平台上该借款人的信用借款上限就是10万元。但是这无法阻止该借款人在n个平台进行借款，承担n x 10万元的债务。小蚁区块链的总账特性可以让P2P借贷平台共享借款人的信用额度。这点与股权众筹平台利用小蚁进行额度控制的原理一致。

最后，使用小蚁登记P2P借贷的债权后，债权变得可转让、可抵押，甚至可编程。债权份额不仅可以在平台内部流转，还能跨平台的进行转让，增加了流动性。债权变得可转让后，长期债权变得更有吸引力。用户可以放心的购买长期债权，享受高息，而无需担心应急之需。通过小蚁的交易转让功能，可以将长期债券贴现转让或抵押贷款。

另外，已经使用小蚁来管理股权的企业甚至还可以利用小蚁来抵押股权，发行企业债。

积分管理

航空公司、运营商、银行、餐饮酒店等许多商业机构都会发行自己的积分。通过给予用户具有使用价值的积分来鼓励留存用户，鼓励多次消费。

这些积分发行机构的数据库都是一个个的数据孤岛（information silo）。A机构无法可信的获得B机构的积分发行情况，因此A、B机构间的积分就难以实现互联互通。通过小蚁区块链发行的积分可以公开透明可信的被任何人查阅，限制了发行人的滥发冲动。用户的交换需求和做市商的做市逐利会形成一个多种积分的交易市场，激活大量沉睡的沉淀积分。

供应链金融

供应链金融涵盖众多业务模式与环节，从保理、贸易金融、仓单融资、应收账款融资到供应链中的企业票据、企业授信融资等不同的金融业务环节。基于区块链技术提供分布式、不可篡改的业务信息记录平台，可以在参与方认证、交易有效性和时效性验证、银行融资调查、企业融资材料等各环节中提供真实有效、低成本的解决方案，从而提升供应链金融整体效能。

其他

小蚁的用户发行资产功能还可以被用来发行基金份额、财产凭证等；电子合同功能还可以被用做证据存证、金融合约等；去中心化的交易功能可以被用作大宗商品交易、外汇交易等。

法律地位

待修订

> 小蚁中没有具备通用的支付、定价功能的原生货币，而是以网关的方式引入人民币等法币。小蚁本身不是一种数字货币，而是一种区块链协议，因此没有货币方面的法律争议，不是五部委《关于防范比特币风险的通知》所指虚拟货币，可以与银行、支付机构合作。

> 小蚁上的个人和组织机构用户均可通过政府授权的CA认证机构进行实名认证。区块链上的股权登记由通过实名认证的公司进行电子签名。股权的转让和交易都由出让人、受让人、公司三方参与签名。公司参与三方签名前有义务保证股权的转让和交易符合《公司法》中“需征得原股东半数同意”、“原股东有优先认购权”、“股东人数限制”等方面的规定。小蚁上的股权转让和交易的本质是一份参与各方都进行电子签名的电子合同。

> 小蚁内置了KYC（用户身份认证）和AML（反洗钱）接口方案。第三方支付、银行等金融机构可以合规的使用小蚁协议。考虑到遗失密钥的可能性，小蚁还设计了一种资产找回机制——即时你遗失了某个地址的对应私钥，你仍然可以无需借助第三方，就能找回其中的资产。

经济模型

系统资产与费用

小蚁中内置了两种系统资产：小蚁股和小蚁币。小蚁股代表小蚁区块链的所有权，用于选举记账，获得小蚁币分红等；小蚁币代表小蚁区块链的使用权，用于支付小蚁区块链的各种系统费用。

系统费用

向小蚁区块链中写入数据需要支付一定的小蚁币作为系统费用，系统费用分为两大类：

- 记账人收取的记账费

  当要向小蚁区块链中写入一笔交易时，该笔交易一般需要包含一定数量小蚁币作为记账费。记账费由记账人收取，用于补贴记账节点的存储、带宽、计算资源支出。

记账费是否收取，收取多少由记账人集体决定。一笔交易可以不包含任何记账费，只要有超过2/3的记账人愿意将这笔交易写入区块链，这笔交易就会被记录于小蚁区块链。因此，需要批量使用小蚁的机构也可以在链外用法币向记账人支付一定费用，而在链内不再提交任何小蚁币作为记账费。

- 小蚁股持有人收取的附加服务费

  附加服务费是指使用小蚁区块链完成某些高级功能而需要用小蚁币支付的费用。目前需要支付附加服务费的交易类型为：资产创设、候选记账人登记。未来将支持的资产变更、资产注销、资产冻结等高级功能也会需要附加服务费。

  附加服务费会按小蚁股的持有比例立即记录到小蚁股的持有地址上。小蚁股持有人在任何时刻都可以进行认领操作，取得这些已经记录在名下的小蚁币。

小蚁股

小蚁股，英文antshare，缩写为ANS。

小蚁股共1亿份，代表了小蚁区块链的所有权。1亿份小蚁股在创世块中一次性被创设出来，并按一定的分配方案进行分配。小蚁股的总量恒定为1亿，不可增加。小蚁股的最小单位为1小蚁股，不可再分割。

小蚁股的主要用途为：

- 投票产生记账人
- 获得新区块生成的小蚁币
- 获得以小蚁币支付的附加服务费
- 投票决定小蚁区块链协议的重大事项

小蚁币

小蚁币，英文antcoin，缩写为ANC。

小蚁币共1亿份，代表了小蚁区块链的使用权。小蚁币会随着每个新区块的生成而产生，依照既定的缓慢衰减的发行速度，经历总量从0到1亿的过程，约22年达到1亿总量。

小蚁币的主要用途为：

- 支付小蚁区块链的记账费
- 支付小蚁区块链的附加服务费
- 作为记账候选人押金

分配与发行

小蚁股的分配机制

1亿总量的小蚁股在创世块中被一次性创设。在创世块运行前小蚁团队将按照一定的规则对小蚁股进行分配。

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%的小蚁股将在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，具体见ICO细则。

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。

早期支持者、ICO 1参与者、ICO 2参与者所分配到的小蚁股都将在小蚁区块链主网运行后立即获得。小蚁区块链主网预计2016年第4季度开始运行。

小蚁币的发行机制

小蚁币伴随着每个新区块的生成而产生。小蚁币初期总量为零，伴随着新区块的生成逐渐增多，直至约22年后达到总量上限1亿。小蚁的每个区块的间隔时间约为15秒，200万个区块约合1年时间。

第一年（实际为0-200万个区块），每个区块新生成8个小蚁币；第二年（实际为第200-400万个区块），每个区块新生成7个小蚁币；以此类推，每年递减1个小蚁币，直至第8年递减至每个区块新生成1个小蚁币；自此保持每个区块新生成1个小蚁币直至约22年后的第4400万个区块，小蚁币总量到达1亿，则停止伴随新区块生成小蚁币。

按照这样的发行曲线，第1年会有16%的小蚁币被创造，前4年会有52%的小蚁币被创造，前12年80%的小蚁币被创造。

这些的小蚁币都会按照小蚁股的持股比例，记录在小蚁股地址上。小蚁股持有人可以在任意时间进行发起一笔认领交易，将这些小蚁币认领到小蚁股的地址上。例如某人持有占全网1%的小蚁股，则在第一年，该用户就能够每个区块获得8/100=0.08个小蚁币，每天获得约460.8个小蚁币。

技术架构

用户

私钥、公钥

私钥：一个256位的随机数，由用户生成并保管且不对外公开。私钥是用户账户使用权以及账户内资产所有权的证明。

公钥：通过一定算法，每一个私钥都有一个与之相匹配的公钥。小蚁中的公钥由私钥通过ECC（椭圆曲线密码学）曲线算法生成。小蚁将支持的ECC类的算法为secp256r1和 SM2（中国商用密码算法）。

脚本、地址

脚本：小蚁使用了类似于比特币的OP_CODE脚本系统。小蚁中的OP_CODE是一套类似于脚本语言的图灵完备的指令集。例如下列两段脚本就都能实现校验多重签名的功能

```
OP_M （公钥列表） OP_N OP_CHECKMULTYSIG


OP_PUSHBYTES M （公钥列表） OP_PUSHBYTES N OP_CHECKMULTYSIG
```

地址：地址是脚本的哈希值。小蚁中地址的形式如下：

```
AM2Y8aSWh3LTwQBoZCNSVNCF9eqVt2vmVX（secp256r1/SHA256算法对应地址）
SSYfWvN36FsWejmGXyhBtP5iKq9EGuaEPr（SM2/SM3算法对应地址）
```

小蚁支持的哈希算法是SHA256和SM3（中国商业密码算法）

账户和账户地址

账户是指一定数量（1-16个）的公钥的组合。最基本的账户由一个公钥组成，其账户地址就是其1-of-1多重签名地址。

更高级的设计中，账户可以由两个公钥组成，这两个公钥所生成的2-of-2多重签名的地址为账户地址。两个公钥中，数值较小的那个为支付公钥；较大的为查询公钥。持有查询公钥对应的私钥（即查询私钥）可以读取该账户所能控制的资产的余额和历史交易信息，持有查询私钥和支付私钥可以支配该账户所能控制的资产。结合小蚁区块链的隐私地址方案，用户可以对外提供一个固定的账户地址作为收款信息，而不会牺牲隐私。

在钱包客户端设计中查询私钥和支付私钥可以分别用查询密码和支付密码加密。用户的体验和使用网银相同，用查询密码登陆，用支付密码支付。

身份认证

用户（个人或机构）可以向CA证书颁发机构申请身份认证，以便于在交易中向其他交易参与方提供真实身份信息。申请认证时，用户向CA提供本人所控制的公钥和身份证明材料，并以对应私钥签名。核实无误后，CA向用户颁发一份数字证书，该证书由CA机构签名，证书内包含了用户的公钥和身份信息。该数字证书证明了该公钥和用户身份间的一一对应关系。

用户在使用小蚁区块链时，以此公钥对应的私钥对交易进行签名。该签名符合中国《电子签名法》中“可靠电子签名”的定义，具备法律效力。

隐私保护

区块链对于数据公开的要求和隐私保护具有一定矛盾，然而通过一些密码学技术可以解决隐私保护问题。

小蚁区块链的隐私保护方案结合了多重签名隐匿地址、加法同态加密等前沿密码学技术。使用小蚁的隐私保护方案后，除了该笔交易的直接参与者，其他第三方都可以验证交易的有效性，但无法知晓该笔交易的参与者身份和交易金额。

多重签名隐匿地址下的交易数据仍然是全部公开的，但每笔交易间不存在可分析的联系性。即使是同一人向你发送了多笔交易，这些交易也会分散在多个毫无联系的地址中，除了你本人没有人能发现或证明这若干个地址属于你。小蚁区块链在BIP63基础上进行了扩展，加入了多重签名和查询私钥的特性，形成了多重签名隐匿地址方案，具体将另文详细详述。

多重签名隐匿地址可以包括用户身份但不能保护交易金额。小蚁使用加法同态加密手段来隐藏交易金额，但又能让网络中的节点验证交易的有效性。小蚁中的其他节点可以验证某笔资产的交易完成后，全网内该资产的余额不变，从而验证该笔交易的金额有效性，而又无需知道具体的交易金额。

资产

小蚁区块链内的资产可以分为系统资产和用户发行资产。系统资产是小蚁区块链协议内部权益的载体，用户发行资产是小蚁区块链协议外的资产或权益的载体。

系统资产

系统资产包括小蚁股和小蚁币。小蚁股代表系统所有权，小蚁币代表系统使用权。小蚁股和小蚁币的具体已在“（二）经济模型”一章中予以说明，不再赘述。

用户发行资产

任意用户均可发行资产。资产经过创设、分发两个步骤生成。创设后，资产登记在小蚁区块链上但实际上并未生成至地址；分发后，资产实际进入地址。

货币：小蚁区块链协议以网关的形式引入外部货币。货币的转账无需接收方签名。股权类资产：股权类资产用作代表有限公司股权（或股份公司股票）的用户发行资产。股权类资产的转让或交易需要接收方签名同意。债权类资产：债权类资产用作代表个人或组织机构的货币性债务。 其它资产：其它类型资产，资产创始人可进行自定义。

交易

交易是指小蚁区块链协议中引起资产的权益或小蚁区块链协议的权益发生变化的事务。小蚁区块链系统内设计了多种类型的交易，每一笔交易都包含输入列表、输出列表、签名列表，以及与交易类型相关的特定数据。

资产相关交易

资产创设：用作创设一种新的用户发行资产。用户可以自己定义资产的类型、名称、总量等，并指定资产的管理员账户。创设资产需要消耗一定数量的登记券作为附加服务费。 资产分发：在资产创设所设定的总量上限范围内，进行从无到有的分配，在任意发行人指定的地址中生成该资产。资产分配可以一次性完成，也可以在任意时间内分批完成。 资产变更、注销、冻结：尚不支持，将在未来版本中支持。

资产流转相关交易

合同交易：指定所有参与方的交易，并可以根据参与交易的资产类型判断是否要求对方确认接受。对手方可以选择确认接受（签名）或拒绝（忽略）。 委托交易：不指定对手方，但指定一个代理人的合同，由代理人负责撮合交易的对手方。“超导交易”即通过委托交易这种交易类型来实现。超导交易的委单数据结构如下：

```
public class Order //委托单
{
    public UInt256 AssetId; //交易物
    public UInt256 ValueAssetId; //价格单位
    public UInt160 Agent; //代理人
    public Fixed8 Amount; //交易总量
    public Fixed8 Price; //交易价格
    public UInt160 Client; //委托人
    public TransactionInput[] Inputs; //交易输入
```

```
    public byte[][] Scripts; //签名列表
}
```

记账相关交易

登记、撤回候选记账人：希望登记为候选记账人的用户，需支付一笔附加服务费，并同时冻结一笔登记券在记账人地址上。候选记账人可以随时动用被冻结的登记券，但如果这么做了，就会丧失记账人资格，需要重新登记成为候选记账人。用户应在登记成为候选记账人之前就做好参与记账的技术准备。候选记账人随时可能被选为正式记账人。选举记账人：详见记账机制

交易费用

交易费用分为记账费和附加服务费，均以小蚁币支付。具体已在“（二）经济模型”一章中予以说明，不再赘述。

记账机制

区块链

小蚁区块链使用类似比特币的区块链来记录数据。

区块链可以被想象成一本账本，每个区块就是这个账本里的一页账目。每页账目里包含了一个预设时间段里的所有交易。小蚁区块链的区块链约每15秒生成一个区块。新区块附加于前一个区块之后，形成一个链的结构。每个区块内包含了15秒内所发生的交易信息，以及其他必要的检索和校验信息。小蚁区块链的区块数据结构如下图示：

```
public class Block //区块
{
    public uint Version; //版本
    public UInt256 PrevBlock; //链接的区块
    public UInt256 MerkleRoot; //交易列表的散列值
    public uint Timestamp; //时间戳
    public uint Bits; //保留字段
    public ulong Nonce; //随机数
    public UInt160 NextMiner; //下一个区块的
}
```

共识机制细节请参考 小蚁共识机制白皮书