小蚁白皮书

基于区块链技术的资产数字化系统

v1.0

2015.9.7

网站：www.antshares.com　邮箱：contact@antshares.com

导读

第 1 章“概述”是对小蚁的高层次描述，适合任何人士阅读。

第 2-7 章为小蚁的技术实现方案的逻辑描述，适合对区块链技术有一定了解的人士阅读。

小蚁为开源系统，遵循 MIT 开源协议。代码托管于：https://github.com/antshares/antshares

目录

1 概述.....6

1.1 什么是小蚁.....6

1.2 什么是区块链.....6

1.3 小蚁的应用场景：.....6

1.3.1 股权众筹.....6

1.3.2 P2P 网贷.....7

1.3.3 员工持股激励.....7

1.3.4 签署电子合同.....7

1.3.5 其他.....8

1.4 小蚁的设计思想.....8

1.4.1 权力的去中心化 vs 事务的去中心化.....8

1.4.2 清算型区块链 vs 日志型区块链.....9

1.4.3 平行金融系统 vs 对接金融系统.....9

1.5 小蚁的特点.....10

1.5.1 合规对接实体金融.....10

1.5.2 去中心化的“超导交易”.....10

1.5.3 熟悉的用户体验：普通用户无需持有小蚁股/小蚁币；使用查询和支付两个“密码”.....11

1.6 法律与合规.....11

2 用户系统.....12
2.1 私钥、公钥、地址、账户、账户地址.....12
2.2 身份认证.....13
2.3 隐私保护——公开地址 vs 隐私地址.....14
3 资产.....15
3.1 原生资产.....15
3.1.1 小蚁股 AntShare，缩写为 ANS.....15
3.1.2 小蚁币 AntCoin，缩写为 ANC.....15
3.2 用户发行资产.....16
3.2.1 货币.....16
3.2.2 股权类资产.....16
3.2.3 债权类资产.....16
3.2.4 其它资产.....17
4 交易类型.....17
4.1 资产相关交易.....17
4.1.1 资产创设.....17
4.1.2 资产分配.....17
4.1.3 资产变更、注销、冻结.....17
4.2 转移、交换资产相关交易.....18
4.2.1 合同交易.....18
4.2.2 委托交易.....18

4.3 记账相关交易.....18
4.3.1 登记、撤回候选记账人.....18
4.3.2 选举记账人.....19
4.4 交易费用.....19
4.4.1 基本字节费.....19
4.4.2 附加服务费.....19
5 记账机制.....20
5.1 区块链.....20
5.2 共识机制——中性记账.....21
5.2.1 中性记账的特点.....21
5.2.2 选举记账人.....22
5.2.3 对区块随机数达成共识.....22
5.2.4 对区块所包含的交易达成共识.....23
5.2.5 对小蚁币分配达成共识.....23
6 分配机制.....24
6.1 小蚁股分配方案.....24
6.2 小蚁币分配机制.....24
7 周边生态.....24
7.1 交易所.....24
7.2 钱包.....24
7.3 众筹、P2P 网贷.....25

8 总结.....25

1 概述

1.1 什么是小蚁

小蚁是基于区块链技术，将实体世界的资产和权益进行数字化，通过点对点网络进行登记发行、转让交易、清算交割等金融业务的去中心化网络协议。

小蚁可以被用于股权众筹、P2P 网贷、数字资产管理、智能合约等领域。

1.2 什么是区块链

区块链是一种以密码学技术为基础，以去中心化的方式，对大量数据进行组织和维护的数据结构。区块链特别适合用作电子现金或数字资产的账本。区块链上的数据全部都附有相关人的数字签名，不可伪造。

此外，区块链还具有完全公开、高可靠性、即时交割、去信任等诸多优点，以区块链技术构建的财务系统相对于中心化的传统金融机构有着压倒性优势。我们认为区块链技术将成为金融网络的主流底层技术。

1.3 小蚁的应用场景：

1.3.1 股权众筹

小蚁可以被用于股权众筹。众筹完成后，初创公司可以用小蚁来管理众多股东的股权，用小蚁提供的去中心化交易机制进行股权交易。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。通过将股权登记在小蚁

区块链上，初创公司能够以“区块链 IPO”的方式获得资金。

1.3.2 P2P 网贷

网贷平台使用小蚁登记 P2P 网贷的债权后，债权变得可转让、可交易，增加了流动性，并且不仅仅局限于本平台用户。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。只要通过小蚁的交易转让系统，可以随时将长期债券贴现转让。

另外，企业还可以利用小蚁发行自己的企业债。

1.3.3 员工持股激励

采用员工持股激励制度的公司可以用小蚁来进行员工持股管理。使用小蚁比自建系统更经济更安全。小蚁的设计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 25%。

1.3.4 签署电子合同

与比特币等基于区块链的支付系统不同，小蚁是一个基于区块链的电子合同系统。用户与用户间通过私钥对合同进行签名，从而完成数字资产的转让交易。实际上，小蚁可以被用于签署任意电子合同。如果合同的标的物是登记在小蚁区块链上的数字资产，那么小蚁可以自动在链上进行程序化交割执行；如果合同标的物为链外的资产，那么合同参与方自行执行即可。即便

是后者情况下，小蚁也消除了签署、保管大量纸质合同的繁琐性，并用数字签名保证了合同的不可抵赖性。

1.3.5 其他

小蚁的用户发行资产功能还可以被用来发行积分点券、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；去中心化交易所可以被用作大宗商品交易、外汇交易等。

1.4 小蚁的设计思想

1.4.1 权力的去中心化 vs 事务的去中心化

财产的支配是一种权力，应当追求自治与去中心化。比特币通过公钥体系和 PoW 工作量证明，实现了财产权利的自治和去中心化。

然而如果按照确定性的规则，以可追究责任的方式，进行没有自由裁量度的简单事务，并不一定需要追求完全的去中心化。比如，开源程序就并不要求每个人都独立编译源代码，而是提供已编译的程序供下载，只需少数人进行编译验证即可。

如果能够将区块链的记账系统设计成一种确定性的，没有自由裁量度的，作恶会留下密码学证据的简单事务，那么这样的记账机制就可以不追求完全的去中心化，从而获得更高的效率。

小蚁中的记账人的权力远小于比特币矿工，记账仅仅是一种确定性的简单事务。通过这样的设计，小蚁可以做到 15 秒左右的清算确认时间。

1.4.2 清算型区块链 vs 日志型区块链

Ripple、Bitshares、Counterparty 等区块链是一种日志型区块链，所有的用户行为都记录进了区块链。例如在基于比特币区块链的 Counterparty 中发送一个挂单指令，要 10 分钟后才能确认挂单成功（还不是成交），并且还要支付比普通转账还高的手续费。

小蚁的设计理念为清算型区块链。简单地说，挂单、撤单等不产生资产变更的日志型交易不需要写进区块链。区块链仅用作登记发生资产变更的交易。清算型区块链牺牲了一部分非关键性的信息记录，但获得了更好的吞吐量、灵活性和用户体验。并且派生除了一种新型的去中心化交易模式——“超导交易”。

1.4.3 平行金融系统 vs 对接金融系统

比特币的 PoW 机制的抗审查性极佳，用户可以匿名的进行转账，矿工可以匿名的进行记账。抗审查性同时带来了合规上的难度。比特币创造了一个独立于实体世界的平行金融系统。然而，平行金融系统难以对接实体世界资产。受实体世界法律约束的股权、债权等难以合规导入。

小蚁的目标用户是整个现存互联网金融生态，需要引入大量实体世界的金融资产。因此小蚁的设计充分考虑了合规要求，定位为一个对接实体世界的区块链金融系统。

1.5 小蚁的特点

1.5.1 合规对接实体金融

与实体世界的兼容性是小蚁追求的目标。

小蚁为个人和公司用户都提供了中国法律认可的身份认证方案。通过身份认证的账户所参与交易的电子签名受中国《电子签名法》的认可和保护，等同于实名签章。身份认证是用户可选项，而非强制项。

股权等资产的转让和交易，其实质是各方签署电子合同，受中国《合同法》认可和保护。

1.5.2 去中心化的“超导交易”

通过一种小蚁独有的去中心化交易机制“超导交易”，用户能够以超越中心化交易所的体验，完成去中心化交易。用户无需给交易所充值，就可以在交易所进行挂单。挂单成交后，交易所将成交的交易信息广播到小蚁协议网络中，并被写入区块链。

例如某用户 A 通过“超导交易”卖出某公司股权，该用户无需把股权事先转入交易所。只需要在本地通过私钥对委托单进行签名，就可挂单。与对手盘成交后，对方的人民币款项将直接进入用户 A 的钱包，无需通过交易所中转。

超导交易所无需管理用户的钱财，没有充值提现流程，简化了运营流程，增加了用户信任度。任何个人和机构都可以成为超导交易所，只要其运行的服务器能提供稳定的撮合服务。

超导交易创造了一种新形态的交易——交易所负责信息的撮合，区块链负责财物的交割。由于不托管用户财物，且交易指令均有密码学证据，超导交易所没有什么特殊的权力，因此监管当局很可能不需要对超导交易所进行前置审批。我们认为随着区块链技术的主流化，超导交易这种模式会成为包括 A 股在内的主流金融市场的发展方向。

1.5.3 熟悉的用户体验：普通用户无需持有小蚁股/小蚁币；使用查询和支付两个“密码”

小蚁链上的买卖交易由“超导交易”交易所完成。用户的挂单、撤单指令本身不消耗小蚁币。挂单成交后，由交易所来支付写入区块链所需的小蚁币手续费。体验和传统股票市场一致，用户无需持有小蚁股/小蚁币。

此外，小蚁的协议设计使得小蚁的客户端可以使用查询、支付两个密码（私钥）。用户体验和传统网银一致，用户学习成本低，同时提供了良好的安全性。

1.6 法律与合规

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。

2 用户系统

2.1 私钥、公钥、地址、账户、账户地址

私钥：一个 256 位的随机数，由用户保管且不对外公开。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：每一个私钥都有一个与之相匹配的公钥。ECC 公钥可由私钥通过单向、确定性的算法生成，候选方案为 secp256r1（国际通用标准）、secp256k1（比特币标准）和 SM2（中国国标）。

地址：将一组公钥的有序排列得到的脚本，通过单向、确定性的算法生成，目前支持的脚本形式有：

OP_M （公钥列表） OP_N OP_CHECKMULTYSIG

OP_PUSHBYTES M （公钥列表） OP_PUSHBYTES N OP_CHECKMULTYSIG

地址的形式如下：

AM2Y8aSWh3LTwQBoZCNSVNCF9eqVt2vmVX（secp256r1 算法对应地址）

36wgQd5KunzhDbgF7eNhm7J5paCWzY2ghj（secp256k1 算法对应地址）

SSYfWvN36FsWejmGXyhBtP5iKq9EGuaEPr（SM2 算法对应地址）

采用其中哪一种还是三种均支持，尚需结合数字证书和身份认证的合作方所提供方案而定。目前已确定至少支持 secp256r1（国际标准）。

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。

2.2 身份认证

用户（个人或机构）可以向 CA 申请身份认证，以便于在交易中向对方提供身份信息。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。（见图 1）

用户在使用小蚁时，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。（见图 2）

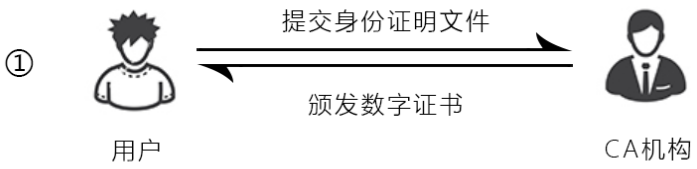


图1：进行身份认证

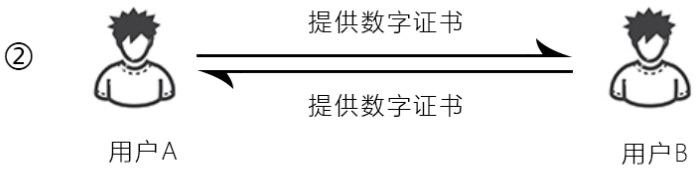


图2：交易时证明身份

包含用户身份信息的数字证书由用户自行保存，不存储在小蚁区块链上。因此，除非用户主动向他人提供数字证书，任何第三方均无法获知其身份信息。除非主动提供，用户的身份和其公钥之间没有对应关系。

2.3 隐私保护——公开地址 vs 隐私地址

数据公开和隐私保护看似矛盾，小蚁使用基于多重签名的 Stealth Address 隐私地址方案很好的解决了此问题。使用隐私地址后，除了该笔交易的直接参与者，其他人都无法知晓该笔交易的参与者身份。

隐私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。

比特币的 Stealth Address 方案为 BIP63 提案。小蚁在此基础上进行了扩展，加入了多重签名和查询私钥的特性，形成了自己的隐私地址方案，具体将另文详细详述。

3 资产

小蚁内的资产可以分为原生资产和用户发行资产。原生资产是小蚁协议内部权益的载体，用户发行资产是代表小蚁协议外的资产或权益的载体。

3.1 原生资产

小蚁内置两种原生资产：小蚁股和小蚁币。

3.1.1 小蚁股 AntShare，缩写为 ANS

小蚁股共 1 亿份，代表了小蚁协议的所有权。在创世块中 1 亿份小蚁股被创设，随后按一定分配方案进行分配。小蚁股总量上限不可增加。

小蚁股的主要权益为：

a) 投票产生记账人

b) 持续获得小蚁币作为系统分红

c) 投票决定小蚁协议的重大事项

3.1.2 小蚁币 AntCoin，缩写为 ANC

小蚁币总量为 1 亿，可精确到 10^{-8}，代表小蚁协议的使用权。小蚁币按

照一定分发曲线在每个区块中持续分配给小蚁股的持有者。小蚁币总量上限不可增加。

小蚁币的分配算法如下：

当前区块的发行数量 = （总量 – 上个块的已发行量）x 2.4297257e-7

小蚁币的主要用途为：

a) 支付小蚁的附加服务费

b) 支付小蚁的基本字节费

c) 作为记账候选人押金

3.2 用户发行资产

任意用户均可发行资产。资产经过创设、分配两个步骤生成。

3.2.1 货币

小蚁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。

3.2.2 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。

3.2.3 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。

3.2.4 其它资产

其它类型资产，资产创始人可进行自定义。

4 交易类型

交易是指小蚁协议中引起资产的权益或小蚁协议的权益发生变化的事务。小蚁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。

4.1 资产相关交易

4.1.1 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小蚁币作为附加服务费。

4.1.2 资产分配

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。

4.1.3 资产变更、注销、冻结

尚不支持，将在未来版本中支持。

4.2 转移、交换资产相关交易

4.2.1 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）。

4.2.2 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
}
```

4.3 记账相关交易

4.3.1 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，并同时冻结一笔小蚁币在记账人地址上。候选记账人可以随时动用被冻结的小蚁币，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。

4.3.2 选举记账人

详见记账机制

4.4 交易费用

交易费用分为基本字节费和附加服务费，均以小蚁币支付。其中，附加服务费会被销毁，成为未分配的部分，参与未来分配；基本字节费则被支付给记账人作为记账奖励。

4.4.1 基本字节费

基本字节费是因交易占用传输带宽和区块链字节所产生的费用。基本字节费和交易的字节数正相关，由记账人收取。记账人可自行决定是否收取以及费率标准。

4.4.2 附加服务费

附加服务费是使用小蚁协议完成某些高级功能而需支付的费用。目前需要支付附加服务费的交易类型为：资产创设、资产变更、资产注销、资产冻结、候选记账人登记。

附加服务费不由任何人收取，而是立即销毁，恢复到未分配的状态，进而最终通过前述小蚁币分配机制，按持股比例再分配给小蚁股的持有人。

5 记账机制

5.1 区块链

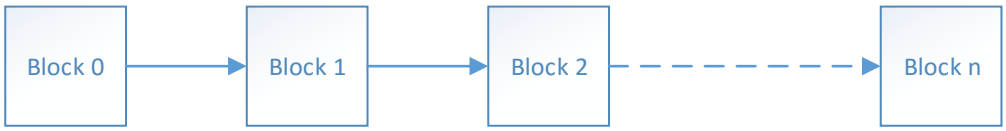
小蚁使用类似比特币的区块链来记录数据。

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; //下一个区块的记账人
    public byte[] Script; //签名
    public Transaction[] Transactions; //交易列表
}
```



一个完整的区块链包含了自创世块以来的所有交易信息，依次执行这些交易就能得到当前的所有资产的归属和状态。

区块链技术的去中心化特点保障了系统的健壮性和安全性；公开数据特

点保证了系统的透明性和可审计性;小蚁区块链可以以极低的成本完成传统中心化数据库的等量事务。

5.2 共识机制——中性记账

共识机制是指运行小蚁协议的各节点对当前区块链状态达成一致意见的机制。

小蚁通过小蚁股持有人投票选举,来决定记账人及其数量;被选出的记账人进行对每个区块内容进行共识，来决定其中所应包含的交易。

5.2.1 中性记账的特点

小蚁的记账机制被称为“中性记账“。

PoW/PoS/DPoS 的出发点是解决“谁有记账权”这一问题。而中性记账则主要解决“如何限制记账人权力“这一问题。在中性记账的共识机制下，记账人只有选择是否参与记账的权力,而不能改变交易数据,不能人为排除某笔交易，不能人为对交易进行排序。

小蚁的中性记账区块链可以做到：

a) 15 秒一个区块，优化后有望达到 5 秒以内

b) 单个记账人不能拒绝包含某笔交易进入当前区块

c) 每个确认由全体记账人参与，一个确认就是完全确认

d) 结合“超导交易”机制，记账人不能通过构造交易来抢先成交牟利（front-running）

5.2.2 选举记账人

小蚁股的持有人可以发起“选举记账人”交易，对选择任意数量个（1-1024 个）候选记账人进行投票支持。我们认为记账人应当实名化，候选记账人应当通过其他信道（如参选网站）提供能证明其真实身份的数字证书。

小蚁协议实时统计所有投票，并计算出当前所需记账人的人数和记账人名单。所需记账人人数算法为：将所有选票按所支持人数排序，按所持小蚁股的权重取中间的 50%，然后取算术平均值。当人数不足最低标准时，将启用系统预置的后备记账人来顶替。

所需记账人人数确定后，按由高到低的得票数确定记账人名单。

1 份小蚁股投给一个候选记账人，计 1 票；1 份小蚁股投给多个候选记账人，各个候选记账人各计得 1 票。

5.2.3 对区块随机数达成共识

每个区块生成前，记账人之间需要协作生成一个区块随机数。小蚁使用 Shamir’s Secret Sharing Scheme（简称“SSSS 方案”）来协作生成随机数。

SSSS 方案通常用于密码共享。通过 SSSS 方案，可以通过密文 S 生成 N 份密文碎片，持有其中的 K 份，就能还原出密文 S。

小蚁记账人（假设为 N+1 个）之间通过 3 步可以对随机数达成共识。

第一步，自选一个随机数，将此随机数通过 SSSS 方案生成 N 份碎片，用其他 N 个记账人的公钥加密，并广播。

第二部，收到其他 N 个记账人的第一步的广播后，将其中自己可解密的

部分解密，并广播。

第三步，收集到至少 K 份密文碎片后，解密出随机数；获得所有记账人的随机数后，合并生成区块随机数。

区块随机数由各个记账人协同生成，只要有一个诚实的记账人参与其中，那么即便其他所有记账人合谋，也无法预测或构造此随机数。

5.2.4 对区块所包含的交易达成共识

在上述区块随机数生成的第一步的广播中，记账人还同时广播其认为应该写入本区块的每笔交易的散列值。其他记账人侦听到广播后，检查自己是否有该交易散列值的对应交易数据，如没有则向其他节点请求。

当区块随机数产生后，每个记账人合并所有第一步广播中的交易（剔除只有散列值但无法获得交易数据的交易），并签名。获得 2/3 记账人的签名，则本区块完成；否则，本区块的本轮共识失败，退回 5.2.3 的第一步再次尝试进行共识。

5.2.5 对小蚁币分配达成共识

每个区块中除了用户发起的交易外还有一笔特殊的交易用于将小蚁币分配给小蚁股的持有人。其算法是根据区块随机数，以持股量为权重，随机发送给小蚁股持股人。每个区块里分配的小蚁币数量详见 3.1.2 所述算法。

6 分配机制

6.1 小蚁股分配方案

用户通过参与众筹、交易所购买、场外转让等方式获得小蚁股。小蚁股代表了小蚁协议这个网络的所有权。

6.2 小蚁币分配机制

创世块中，无人持有小蚁币。随后根据一定算法，每个块向小蚁股的持有者按比例概率分配小蚁币。具体的分配机制详见 3.1.2 所述。

7 周边生态

7.1 交易所

小蚁股和小蚁币可以在例如火币、OKCoin、比特币中国、比特时代这样的中心化交易所交易，也可以在小蚁的区块链上以超导交易的形式交易。

目前交易所的大量成本耗费在资产和货币的充值提现上。超导交易所不需要参与资产的交割，大大减轻了运营成本。详见前文 1.3.2“超导交易“。

7.2 钱包

钱包服务商可以通过默认设置，来鼓励小蚁股的持有人选举钱包服务商成为记账人。记账人可以获得小蚁币（基本字节费）作为经济回报。为钱包服务商运营好钱包服务提供了额外的经济激励。

7.3 众筹、P2P 网贷

中国的股权众筹监管意见已明确不允许众筹平台自营股权交易系统。众筹平台可以使用小蚁作为其平台众筹项目的股权管理系统，即满足了用户的转让、交易需求，也合乎监管规定。

同理，网贷平台也可以使用小蚁作为其平台网贷项目的债权管理系统。

8 总结

小蚁使用了区块链技术来完成了资产的注册登记、转让交易、清算交割。通过将资产数字化，使得任意实体资产的财产权益变成可编程化。通过区块链技术的原子级交易和实时交割特性，极大缩减了证券交易的营运成本和生态链条。我们相信小蚁不仅相对于传统金融系统具有压倒性的优势，还将创造出全新的数字化金融生态。