蚂蜂币白皮书

序言：人人生而平等，人人皆能免费挖矿。

蚂蜂币，区块链自挖矿系统。币圈众多大佬幕后支持，技术成熟，公司化运作，倡导绿色环保，公平分发。新人进群：606512783，有一次性奖励 1000 蚂蜂股（矿机），本周在群内有签到或者发言的，每周日根据群聊等级奖励数量不等的蚂蜂股（矿机）。推荐 1 有效用户（领币成功） 奖励 300 蚂蜂股（矿机）。群成员每周有工资蚂蜂股(矿机)和拍卖活动。

群满以后去 bitcointalk.org 论坛进行签名送蚂蜂股（矿机）活动。

蚂蜂币介绍

快捷稳定的支付和交易媒介

蚂蜂系统是一个去中心化的资产和 dapp 应用平台

是一个分布式的智能合约网络服务商

基于拜占庭容错算法的密码学货币，90%免费分发

关于货币

名称：蚂蜂币

简称：MFB

总量：1 亿个

共识算法：dBFT

区块时间：15~20 秒

创新：匿名、跨链、去中心化资产平台

在区块链资产平台提供大零币的安全协议层，能让隐私得到保护，关注隐私的智能合约平台是区块链发展的趋势。

跨链协议能与其他区块链资产进行交易。

基本概览

1、匿名性

2、跨链技术

3、去中心化资产平台

4、公有链

5、格密码学签名与加密技术

蚂蜂币的产生

蚂蜂币可挖 22 年，第一年每个块产出 8 个币，每天产出约 4 万币，平均分配给 1 亿台矿机，也就是说第一年 2500 台矿机每天可挖到一个币。

阶段	每块挖出	每年块数	年数	总产出
1	8	2000000	1	16,000,000

1	7	2000000	1	14,000,000
1	6	2000000	1	12,000,000
1	5	2000000	1	10,000,000
1	4	2000000	1	8,000,000
1	3	2000000	1	6,000,000
1	2	2000000	1	4,000,000
1	1	2000000	1	2,000,000
1	1	2000000	1	2,000,000
1	1	2000000	1	2,000,000
1	1	2000000	1	2,000,000
1	1	2000000	1	2,000,000
1	1	2000000	1	2,000,000
1	1	2000000	1	2,000,000
1	1	2000000	1	2,000,000
1	1	2000000	1	2,000,000
1	1	2000000	1	2,000,000
1	1	2000000	1	2,000,000

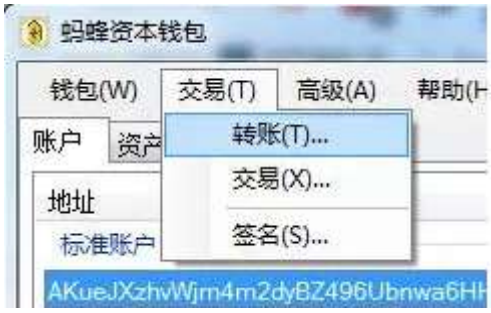
1	1	2000000	1	2,000,000
1	1	2000000	1	2,000,000
1	1	2000000	1	2,000,000
1	1	2000000	1	2,000,000
				100,000,000

提取蚂蜂币

蚂蜂股（矿机）自动生成蚂蜂币，需要手工提前至钱包才能用于交易

具体操作步骤如下

1、点击转账



2、发送资产给自己

3、点击高级提取蚂蜂币

蚂蜂币算法 dBFT 介绍

授权拜占庭容错（dBFT）

蚂蜂区块链是一个分布式的智能合同平台，采用了拜占庭容错委托（dBFT）。它具有两个区块链接参与者：专业节点运算符，称为记账节点，通过运行节点赚钱，以及用户。支持者声称 dBTF 在区块链技术中提供更好的安全性。

专门的记账节点“通过委托投票，在 dBFT 区块链中实现共识”。为

了批准区块链的新版本，需要在节点之间通过三分之二的审批。支持者说，这个系统可以防止分叉事件的发生，对区块链系统的进行彻底的改革。

DBFT 全称为 Delegated Byzantine Fault Tolerant，是一种通过代理投票来实现大规模节点参与共识的拜占庭容错型共识机制。蚂蜂矿机持有者通过投票，可以选出其所支持的记账人。随后由被选出的记账人团体通过 BFT 算法，来达成共识并生成新的区块。投票在蚂蜂网络持续实时进行，而非按照固定任期。

DBFT 对由 n 个共识节点组成的共识系统，提供 f= (n-1)/3 的容错能力，这种容错能力同时包含安全性和可用性，可以抵抗一般性故障和拜占庭故障，并适用于任何网络环境。DBFT 具有良好的最终性，一个确认即最终确认，区块无法被分叉，交易也不会发生撤销或回滚。

在 蚂蜂的 dBFT 共识机制下，每 15~20 秒生成一个区块，交易吞吐量实测可达到约 1000tps，在公有链中性能优秀。通过适当优化，有能力到达 10000TPS，可以支持大规模的商业化应用。

dBFT 结合数字身份技术，使得记账人可以是实名的个人或机构。从而使得冻结、撤销、继承、找回、司法判决过户等非常规操作成为可能。这有利于合规性金融资产在蚂蜂网络中的登记发行。蚂蜂网络计

划在必要的时候支持此类操作。

dBFT 的特点

dBFT（delegated BFT）是一种通用的共识机制模块，提出了一种改进的拜占庭容错算法，使其能够适用于区块链系统。

是基于区块链技术的一种协议。用户可以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。小蚁上可以发行中国《合同法》、《公司法》认可的公司股权，不仅是数字货币圈，还包括主流互联网金融。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。

这种共识机制是在 Castro 和 Liskov 提出的“实用拜占庭容错算法”（Practical Byzantine Fault Tolerance）的基础上，经过改进后使其能够适用于 区块链系统。拜占庭容错技术被广泛应用在分布式系统中，比如分布式文件系统、分布式协作系统、云计算等。dBFT 主要做了以下改进：

1)将 C/S 架构的请求响应模式，改进为适合 P2P 网络的对等节点模式；

2)将静态的共识参与节点改进为可动态进入、退出的动态共识参与节点；

3)为共识参与节点的产生设计了一套基于持有权益比例的投票机制，

通过投票决定共识参与节点（记账节点）；

4)在区块链中引入数字证书，解决了投票中对记账节点真实身份的认证问题；

为什么最终采用一种这样的方案？

答：区块链作为一种分布式账本系统，其内部的经济模型决定了，每一位参与者都可以无需信任其他的参与者，即所谓的去信任。拜占庭将军问题正是描述了参与者之间如何在去信任的情况下达成共识，而拜占庭容错技术正是解决此类问题的方法。此外，区块链的网络环境非常复杂，会面临网络延迟、传输错误、软件错误、安全漏洞、黑客入侵等问题，还有各式各样的恶意节点，而拜占庭容错技术正是可以容忍这些错误的方案。

共识机制跟 PoW、PoS、DPoS 这些相比，优缺点是什么？

答：PoW 即工作量证明，这是一种非常巧妙的方法，它的优点是：

1)算法简单，容易实现；

2)节点间无需交换额外的信息即可达成共识；

3)破坏系统需要投入极大的成本；

它的缺点也非常明显：

1)浪费能源；

2)区块的确认时间难以缩短；

3)新的区块链必须找到一种不同的散列算法，否则就会面临比特币的算力攻击；

4)容易产生分叉，需要等待多个确认；

5)永远没有最终性，需要检查点机制来弥补最终性；

PoS 即权益证明，它将 PoW 中的算力改为系统权益，拥有权益越大则成为下一个记账人的概率越大。这种机制的优点是不像 Pow 那么费电，但是也有不少缺点：

1)没有专业化，拥有权益的参与者未必希望参与记账；

2)容易产生分叉，需要等待多个确认；

3)永远没有最终性，需要检查点机制来弥补最终性；

DPoS 在 PoS 的基础上，将记账人的角色专业化，先通过权益来选出记账人，然后记账人之间再轮流记账。这种方式依然没有解决最终性问题。

dBFT 机制，是由权益来选出记账人，然后记账人之间通过拜占庭容错算法来达成共识，这种方式的优点是：

1)专业化的记账人；

2)可以容忍任何类型的错误；

3)记账由多人协同完成，每一个区块都有最终性，不会分叉；

4)算法的可靠性有严格的数学证明；

缺点：

1)当有 1/3 或以上记账人停止工作后，系统将无法提供服务；

2)当有 1/3 或以上记账人联合作恶，且其它所有的记账人被恰好分割为两个网络孤岛时，恶意记账人可以使系统出现分叉，但是会留下密码学证据；

以上总结来说，dBFT 机制最核心的一点，就是最大限度地确保系统

的最终性，使区块链能够适用于真实的应用场景。

其他功能

数字资产+虚拟世界+智能合约

区块链本质是一个去中心化的分布式账本数据库,其价值在于使用密码学算法产生的一串数据块,时间有序不可篡改,每个数据块中包含多次交易有效确认的信息,由此建立共识机制,从而实现去中心信任体系。利用去中心化、不可伪造、公开透明、分布式记账、不可篡改、智能合约等特点，使得无需中介的价值转移成为可能。

但是区块链不是数据库，主要解决的问题是多方的互信问题，无需把大量数据存储在区块链上。

区块链是一个试图自带信任化和防止篡改的分布式记账系统，打造一个彼此信任的基础设施。
区块链技术将在金融和信息领域占据一席之地。

代币是由区块链记录的解决去中心化和去信任问题，通过加密的算法传输，基于虚拟或特定环境流通与应用的支付手段。

蚂蜂采用七层架构：

数据层：区块+链表结构

网络层：分布式 p2p 网络

共识层：dBFT

激励层：MFB 生产机制

匿名层：零知识证明机制

合约层：智能合约虚拟机

应用层：SDK+合约模板

协议分为底层+中间层+业务层

底层包含数据层、网络层、共识层、激励层

底层支持 UTXO 模型，动态区块大小，15 秒极速确认，无法回滚交易。

中间层匿名层、合约层，采用 Zcash(ZEC)所使用的完全匿名零知识证明机制，达到小额至超大额资产交易，保证隐私不被侵犯，合约层采用高性能虚拟机通过初始合约和控制合约相结合，使得合约具备图灵完备性。

应用层，对移动多终端支持友好，方便开发资产管理应用，dapp 应用，通过官方公布的合约模板，快速部署执行合约。

核心目标：

通过免费的分发股份，公平挖矿，通过提供稳定的客户端，快捷的转账和交易速度，在密码学货币领域支付和交易环节提供可靠的交易媒

介。

主要创新：

人人免费挖矿，人人皆可参与制造货币。

区块链自挖矿系统，杜绝作弊。

经济模型：

免费领取蚂蜂股（矿机）

蚂蜂股（矿机）通过区块自挖矿系统自动生成蚂蜂币

绿色挖矿，公平分发。

业务模型：

前期以蚂蜂币计价，通过拍卖少量蚂蜂股（矿机），带动蚂蜂币流动，产生较为稳定的共识和价值。

后期通过交易所，稳定币价和上涨。

最后，在密码学货币支付和交易环节中发挥巨大的作用。

运营模型：

社区运营，通过成立基金会，吸引区块链人才加入。

通过投票运行主节点，获取交易手续费，保障主节点的去中心和可持续性。

数据结构：

蚂蜂区块链存储透明的交易账本，在蚂蜂区块链上可以发行各类去中心的资产，各资产管理商可以提供承兑业务。

去中心化交易所:

蚂蜂钱包实现了去中心交易所的三次握手交易功能。

共识机制：

dBFT 算法共识。

去中心投票共识。

社区意见共识。

虚拟机：

蚂蜂区块链提供虚拟机，可以发布较为复杂的智能合约。

接口对接：

蚂蜂区块链运行命令行版本可以提供 API 接口和操作说明，方便程序对接。

应用场景：

价值转移的支付和交易环节。

对赌，区块链存储，跨链，彩票，预测等智能合约的实现场景。

常见问答:

为什么要免费分发?

像一切有价值的代币，都应该的免费的,类似早期的比特币。

但是自从比特币出现 ASIC 矿机以后，离公平挖矿的道路越走越远。

为什么要挖矿?

挖矿解决的是公平分发的机制，通过挖矿需要时间来产出币，人人都有机会参与。

蚂蜂币的优势在哪里?

1、 绿色挖矿，免费领取蚂蜂股（矿机），一经发放，无需开电脑，无需打开钱包，自动挖矿，保证了区块链精神，做到了真正的公平公正公开。

2、 独立的公链平台，可以发布资产代币，各个资金直接可以互相交易。

3、 转账速度快，区块时间 15 秒。

4、 高可靠性，1 个区块就可确认。

5、 超低交易手续费。

6、 总量固定，最多只能挖出 1 亿个。

7、 安全性强，自由控制资产。

8、 高稳定性，使用自建区块链，能承受每秒上万笔的交易。