三易社：致力于交易保护、行业应用的区块链服务平台

**概述**

三易社基于区块链技术，结合传统易理文化，吸取现行主流区块 链的先进技术，组建一个去中心化、有智能合约功能的公共区块链， 实现多链协同和产业应用服务平台。

**引言 [1]**

区块链（Blockchain）是一种由多方共同维护，使用密码学保证 传输和访问安全，能够实现数据一致存储、难以篡改、防止抵赖的记 账技术，也称为分布式账本技术（Distributed Ledger Technology）。 典型的区块链以块-链结构存储数据，比特币就是基于区块链技术开 发的加密数字货币。

比特币出现之后，莱特币、零币、PPCoin、Ethereum 等数字货币 如雨后春笋般涌现出来，这些加密货币实验或许将促进人类货币体系 的进一步发展。

随着以比特币为首的数字货币受到越来越多的关注，人们开始将 区块链技术应用到金融领域，为区块链系统引入“智能合约”技术。

智能合约是一种通过计算机语言实现的旨在以信息化方式传播、 验证或执行合同的计算机协议。智能合约技术对区块链的功能进行了 拓展。自此，区块链发展进入第二阶段：可编程金融。有了智能合约 系统的支持，区块链的应用范围开始从单一的货币领域扩大到涉及合

约共识的其他金融领域，区块链技术得以在股票、清算、私募股权等 众多金融领域崭露头角。随着区块链技术的进一步发展，其“开放透 明”、“去中心化”及“不可篡改”的特性在其他领域逐步受到重视。 各行业专业人士开始意识到，区块链的应用也许不仅局限在金融领 域，还可以扩展到任何需要协同共识的领域中去。于是，在金融领域 之外，区块链技术又陆续被应用到了公证、仲裁、审计、域名、物流、 医疗、邮件、鉴证、投票等其他领域，应用范围逐渐扩大到整个经济 社会。除此以外，人们还试图将区块链技术应用到物联网中，实现人 与人、人与机器的万物互联。整个社会将逐渐进入智能互联网时代， 最终形成一个可编程的社会。

**技术框架**

各类区块链虽然在具体实现上各有不同，但在功能架构存在一定共性。三易社以中国信通院发布的《区块链白皮书（2019）》[2]中提出通用型的区块链系统技术架构为基础，将区块链的功能架构划分为基础设施、基础组件、账本、共识、智能合约、接口、应用、操作运维和系统管理等模块。

接口

交易、行业服务

基础设施

系统管理

智能合约

共识

账本

基础组件

运维操作

基础设施层：为上层提供物理资源和计算驱动，是区块链系统的物理支持；

基础组件层：为区块链系统网络提供通信机制、数据库和密码库；

账本层：负责交易的收集、打包成块、合法性验证以及将验证通过的区块上链；

共识层：负责协调保证全网各节点数据记录一致性；

智能合约层：负责将区块链系统的业务逻辑以代码的形式实现、编译并部署，完成既定规则的条件触 发和自动执行；

接口层：主要用于完成功能模块的封装，为应用层提供简洁的调用方式；

系统管理层：负责对区块链体系结构中其他部分进行管理；

操作运维层：负责区块链系统的日常运维工作。

**多链协同**

随着区块链系统运行，存储总量的不断增加，区块链存储及节点 的可扩展性问题逐渐凸显。为解决这一问题，系统通过多链融合和跨 链协同操作实现区块链系统的可扩展，如同构多链和异构多链，保证 区块链的可追溯性。

三易社前期提供公共账单链和货币状态链，公共账单链记录全网 交易和持币信息，货币状态链记录对应货币合成信息和当前的持有状 态信息。后期开发各类上层应用，增加相应侧链，丰富平台功能。

**混合共识**

为了保证区块链在交易吞吐量与共识节点数上同样可扩展性问 题，系统采用混合共识，组合工作量证明共识（POW）和权益证明共识（POS），结合两者优点并平衡彼此弱点来提升共识的效率和安全性。

在项目的早期阶段使用PoW ，经过一段时间的发展，股权分布相对分散以后，选择“ PoS+ ”共识机制。

**x11算法**

 X11是一种广泛使用的哈希算法，其与其它算法不同，称为链接运算。 X11由11 轮SHA3算法组成，每轮哈希计算的结果都被提交到区块链的下一轮计算去。使用多轮算法，可以减少专门为数字货币挖矿设计的ASIC使用的概率。

在比特币发明后，爱好者开始使用CPU来挖矿，不久之后是使用GPU软件快速取代了CPU。几年后ASIC即是专用集成电路被研发出来，迅速取代了GPU进行挖矿。

考虑到专门为X11算法而设计的ASIC矿机的复杂性和机器制造的困难性，我们预计这将需要比比特币更多的时间进行研发，这就允许爱好者有更长的时间参与挖矿。我们深信这对均与的分配和数字货币的成长起着极其重要的作用。

跨链哈希运算的另一个好处是高端的CPU有着跟同级GPU接近的平均回报。GPU消耗的功率已有30-50%的下降，比大多数加密数字货币使用的Scrypt算法的功率少得多。

**多重认证**

ASIC 即是专用集成电路被研发出来用于挖矿后，同时各类矿厂应 时产生，造成算力聚集，也提高了参与门槛，让一般玩家失去入场的 信心，也与去中心化的核心背道而驰。另外，算力聚集达一定程度， 可产生篡改账本的可能。

三易社一方面邀请一定量的可信任且受认证节点参与全账本记 账，保证一定基数的正确节点；一方面对节点和钱包进行双认证加密， 从逻辑和技术上抑制大型矿厂的产生，最大程度上保障最多数玩家的 利益。

**节点分类**

系统网络中的每一个节点都是经过认证后才生效，每个节点都具

独立不重复的 ID，系统按不同规格对节点进行分类：主节点和次节

点。

主节点是运行在 p2p 网络上的服务器，让次节点使用它们来接受

来自全网的动态变化。这些主节点需要消耗一定的网络和能源，来保

证网络的正常运作。所以，这些主节点对系统网络而言就十分重要，

它们能让客户端同步和通过全网快速广播信息。因为这些节点将具有

高可用性，而且在为网络提供符合一定要求的服务。所以主节点能够

获得一定比例服务奖励。

### 主节点权益

主节点使用一系列扩展协议在全网进行广播，包括主节点消announce 机制和主节点消息 ping 机制。这两类机制用来确认主节点处于生效状态，除了它们，执行服务量证明机制需求的还Darksend

和 InstantX。所以，运行主节点需要成本，这在网络上创建了生效

节点的硬限制和软限制。

主节点认证生效条件是与之绑定钱包里的 SYB 不低于 168 枚，而系统的每一枚币都是通过“挖矿”产出。而系统又需要一定量的主节点来维持动作，所以在前期货币数量不足的情况，系统前期会进行一定数量的主节点预认证。

主节点经认证生效后，它可为全网的客户端提供服务，参与平台

相关政策表决，均享平台服务收益，同进还以利息的形式获取奖励。

主节点和次节点获取的收益是来自同一个矿池，其中大约有 30%的区块奖励由主节点享受。

考虑到主节点奖励计划的奖励率是固定的百分比，还有有效主节

点存在一定的波动，所以主节点奖励会根据当前生效的主节点总数作

出相关调整，计算方式 如下：(n/t) \* r \* b \* a

n: 运行者控制的主节点数，人均控制 5 个以内；

t: 主节点的总数；

r: 当前主节点的区块奖励总数；

b: 平均每天的区块数；

a: 主节点的平均奖励基数；

**主节相关说明**

在钱包中发送 168SYB 到特定地址，激活代码后，经网络验证生成能在全网进行广播的主节点， 随之次级私钥生成，它是用来对其它所有信息进行签名，另外在运行单机模式时还可用来完全锁定钱包。

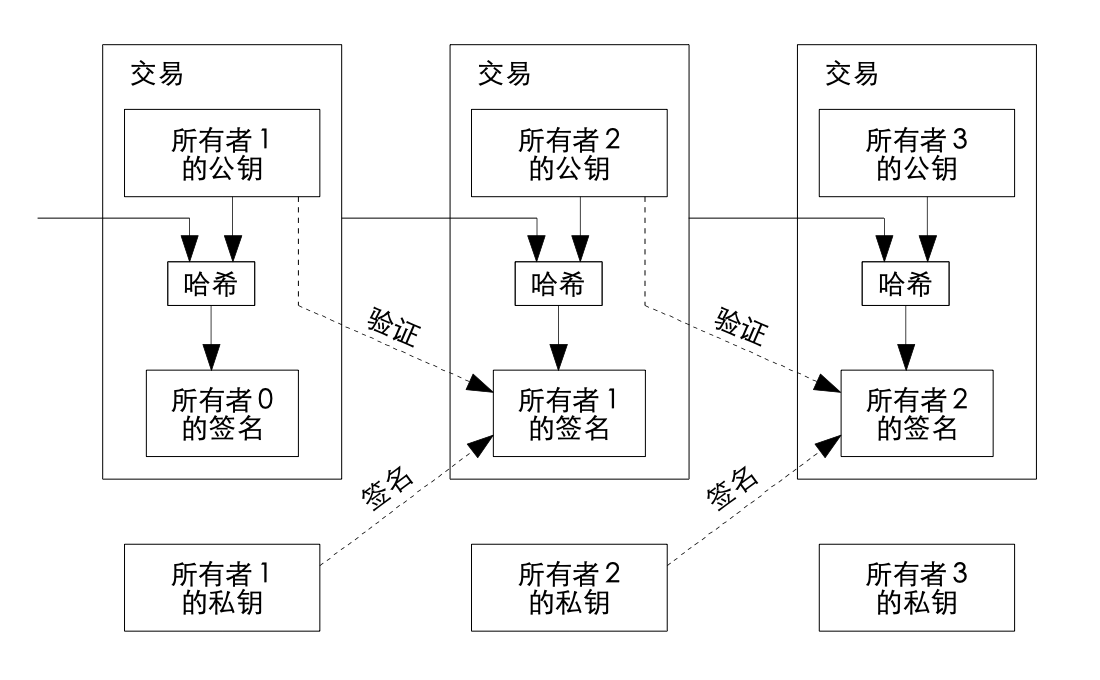
在两台独立的机器上使用次级私钥让冷模式成为可能。主要的“热”客户端对 168SYB 的输入进行签名，此过程包含使用二级私钥 对信息进行签名。 之后，“冷”客户端能发现包含次级私钥的信息 并将主节点激活。这让“热”客户端失效（客户端关闭），这样攻击 者访问激活后的主节点也不可能获得窃取其中的 168SYB。

主节点开始运行时，会向全网发送“主节点广播”信息，包含有： 信息：（168SYB 输入，可访问的 IP 地址，签名，签名时间，含 有 168SYB 的公钥，次级公钥，用于捐赠的公钥，捐赠的百分比） 此后每隔一段时间，一条 ping 信息会对外发送，证明节点生效中。 信息：（168SYB 的输入，签名（使用次级私钥），签名时间） 随着时间的推移，网络会移除失效的节点，让该节点不再被客户 端利用或再用于服务。节点也可以不停地 ping 网络，但如果它们的 端口不打开，最终会被标记为失效状态，不再用于服务。

**交易方式**

1、一般交易模式 （参考比特币交易[3]）

我们定义一枚电子货币就是一条数字签名链。每个拥有者都通过将上一次交易和下一个拥有者的公钥的哈希值的数字签名添加到此货币末尾的方式将这枚货币转移给下一个拥有者。 收款人可以通过验证数字签名来证实其为该链的所有者。



针对双重花费问题。交易必须公开发布，我们需要一个系统的每个参与者，都同意一个它们已经接受到的单一的订单历史。收款人需要通过主要节点认同它们已经第一时间收到了这笔交易来证明每一笔交易。时间戳服务器，一个时间戳服务器对一组已经被时间戳标示过的数据块进行哈希加密，然后广泛公开发布这个哈希。每个时间戳包含了上一个交易的时间戳在它的哈希里，以后每次交易的时间戳都对上一个进行了加强，以此形成了一个链。每个币都有唯一的时间戳，较早的交易将被视为合法付款。一枚币，一次付款。将相同的币发送给第二个人将显示不同的时间戳，该时间戳发生在时间轴的后面。这会使第二笔付款/交易无效。

2、混币交易模式 （参考达世币匿名交易[4]）

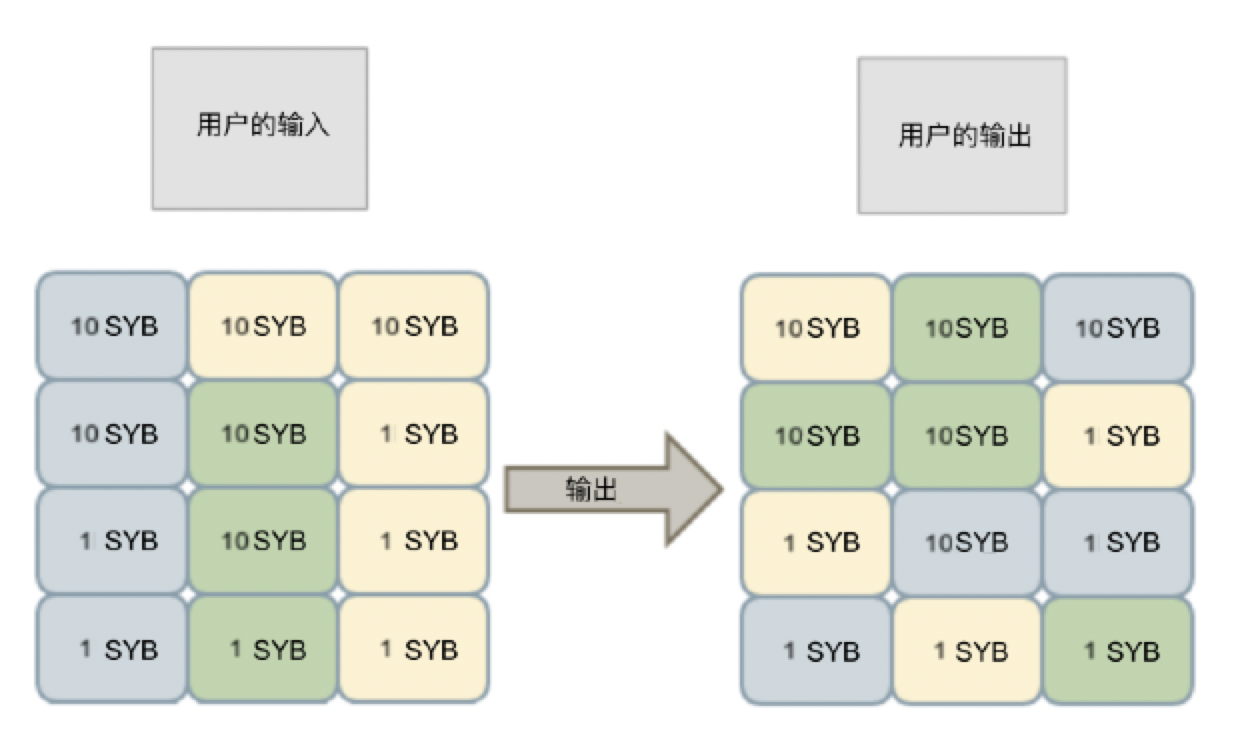
混币交易服务旨在提高交易的匿名性，须发起多笔交易后才能进

行混币交易。

1. 匿名发送首先将你的交易输入打乱面额化。这些面额包含0.001, 0.01, 0.1, 1 和 10 SYB – 就像日常使用中的纸币一样。
2. 然后你的钱包会将需求发送到网络中的特殊节点上，称之为主节点服务器。这些主节点会接到通知你有兴趣混合一定的面额。不会有可识别的信息发送给主节点，所以主节点也不会知道你是谁。
3. 当有其他两个人发出了类似的信息，显示他们也希望混合同样的面额时，混币便开始了。主节点将币混在一起，并给这三个用户的钱包指令，让它们把这些现在已经转化了的币回付给自己。你的钱包将这些面额直接付给自己，但是地址已经改变(称为变更地址)。
4. 为了彻底模糊你的资金，你的钱包必须重复每次面额化过程数次。每次过程完成称为一”轮“。每轮匿名发送将指数级加大追踪你资金来源的难度。用户可选择 1-16 轮混合。
5. 您的资金将至少混合您指定的回合数+最多3个额外回合。
6. 这个混合过程在后台进行，无需您的任何干预。当你希望进行私人交易时，你的资金就可以使用了。无需额外的等候。

注意匿名支付的交易都会取整数，所以所有的交易输入都会被使用。任何超出部分都会被用于交易手续费。

重要：你的钱包只能含有1000个“变更地址”。每一次混币发生，一个变更地址便会被用掉。一旦他们全部被用掉，你的钱包就必须创建更多的地址。但是，你只有让自动备份生效，才可以做到这一点。同样的，如果用户让备份失效，匿名支付失效。



3、快捷交易模式

只对保存相关币链文件的交易申请有效，快捷交易更多是转移币

链并变更币链中的持有记录信息，同时开行全网广播报备，由其它节

点打块。

传统的去中心化加密数字货币都要等上一段时间，通过足够多的区块广播来保证交易是不可撤消的，并且验证这些币没有在别的地方已经被花掉而产生双重花费的可能。这个过程很费时，通常被广泛接受的六步确认会花上15分钟到1个小时不等的时间。其它的加密数字货币都是通过网络上不同程度的中心化处理来实现交易确认时间加速。

SYB凭借其主节点的第二层网络而不受这些限制。 主节点定期形成投票定额，以检查提交的交易是否有效。 如果有效，则主节点“锁定”交易的输入并将此信息广播到网络，有效地保证交易将被包含在后续挖掘的块中，并且在确认时间段内不允许这些输入的任何其他支出。

**挖矿与供应**

SYB 的最小单为币基，共分为 8 类。每枚 SYB 由 8 个币基组合而成，每枚币的币基组合情况不同，不同的币基组合顺序就是相应的数币标识，确保了数币的唯一性和有限性，理论上总币量为 8^8 即为 16777216 枚数币。

币的标识信息是构成币链的主要内容，而每个币基都是网络节点通过“挖矿”产生，节点对应的钱包收集 8 个币基后就可以组成与现有币不重复标识的新币，整个过程就类似一个“铸币”过程。

SYB 每 4 分钟进行全网记账并奖励，逐年减半，预计在 8 年完成所有币基产出和数币合成。第一年每次奖励 512 个币基，理论上可以合成 64 枚 SYB，一天可以产出 23040 枚币；以后逐年减半，直至所有 SYB 产出。相关数据如下表：

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 日期 | 币基数量/次 | 预计合成币量/次 | 预计合成币/小时 | 预计合成币/日 | 预计合成币币/年 | 备注 |
| 第一年 | 512 | 64 | 960 | 23040 | 8409600 |  |
| 第二年 | 256 | 32 | 480 | 11520 | 4204800 |  |
| 第三年 | 128 | 16 | 240 | 5760 | 2102400 |  |
| 第四年 | 64 | 8 | 120 | 2880 | 1051200 |  |
| 第五年 | 32 | 4 | 60 | 1440 | 525600 |  |
| 第六年 | 16 | 2 | 30 | 720 | 262800 |  |
| 第七年 | 8 | 1 | 15 | 360 | 131400 |  |
| 第八年 | 8 | 1 | 15 | 360 | ———— |  |

**发展方向**

区块链通过点对点的分布式记账方式、多节点共识机制、非对称 加密和智能合约等多种技术手段建立强大的信任关系和价值传输网 络，使其具备分布式、不可篡改、价值可传递和可编程等特性。目前， 区块链的技术的应用场景不断铺开，从金融、产品溯源、政务民生、 电子存证到数字身份与供应链协同，场景的深入化和多元化不断加 深。然而，区块链的应用仍旧处于较为初级的阶段，各类应用模式仍 在发展中演进，仍需持续探索。

SYB 主发的发展方向在数字资产和支付、智能合约服务和平台应用：

1. 数字资产和支付：类似常见数字货币一样，可以作虚拟资产投 资，也可以用于各类支付；
2. 智能合约平台，主要提供底层平台，来让开发者在它上面去实 现运用。比如说实现 P2P 交易、电子合同、租赁协议，确保双方交易 双方权益；

3、平台应用，范围非常广，可向金融、社交、游戏、产品跟踪等 方向方向发展。

## **参考链接**

[1] 中国信通院，“区块链即服务平台BaaS白皮书（1.0版），

”<https://www.fxbaogao.com/detail/299027>, 2019.

[2] 中国信通院，"区块链白皮书"  
<http://www.caict.ac.cn/kxyj/qwfb/bps/201911/P020191108365460712077.pdf>, 2019

[3] 中本聪， "比特币：一种点对点式的电子现金系统，"  
<https://bitcoin.org/files/bitcoin-paper/bitcoin_zh_cn.pdf>, 2008.

[4] 达世币匿名支付：[https://docs.dash.org/zh\_CN/stable/introduction/features.html#privatesend](https://docs.dash.org/zh_CN/stable/introduction/features.html" \l "privatesend)，达世币白皮书<https://github.com/dashpay/dash/wiki/Whitepaper_zh_cn>