

星际链 Interstellar chain

白皮书

穿越智能资产，支持星际间大规模贸易的记账

包括未来星际土地的拍卖、转让

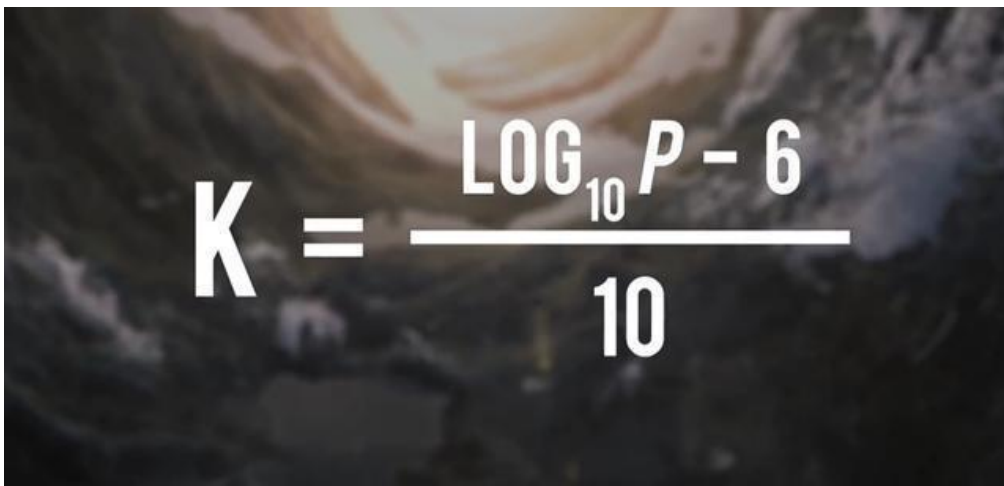
2017 年 11 月 6 日

目录

1. 序言	1
2. 星际链 Interstellar chain	3
什么是星际链	3
ISC (星际币) - 星际链的代币	3
ISC 参数及发行方式	3
关于团队	3
星际链的优势	4
3. 技术部分	5
共识算法	5
POW 机制	5
HBTH-DPOS	5
新的交易类型	6
跨链虚拟机	7
4. 潜在风险及考虑	8
5. 免责声明	9
6. 结论	11

序言

人类从远古蛮荒时代进化到现代文明无需万年，从非洲开始直至扩展到整个地球，这一切都发生在眨眼间，一些 150 年前无法想象的目标都已实现。目前人类已经能够登陆月球，并计划于 2030 年登陆火星，1977 年发射的旅行者一号空间探测器已飞出太阳系，随着科技的进步，人类将很快脱离地球制约并向星际空间探索和发展。


$$K = \frac{\text{LOG}_{10} P - 6}{10}$$

1963 年苏联宇宙学家尼古拉·卡尔达肖夫（Nikolai S. Kardashev）创造了一个衡量宇宙文明等级的指数-卡尔达肖夫指数，卡尔达肖夫指数对于文明先进程度的评估主要基于该文明可以利用的能源等级及总量，通过这种方式 3 种基本的文明程度被定义出来。

一级文明，被称为行星文明，这种文明和目前的人类文明很相似。这种文明等级可以储存和利用所用从主恒星到达行星的能量，对我们来说，主恒星就是太阳——来自太阳的能量达 7×10^{17} 次方瓦。目前地球文明还不能完全达到一级文明，我们处于一个扩展的文明级别：零型。

卡尔达肖夫表示，人类正在经历技术发展的青春期，这是典型的将要进入一级文明的过程。科学家认为人类在未来的 100 年会进入一级文明；

星际贸易在未来的 100 年后将成为现实：星际间的土地、能源、矿藏以及知识技术的交易会变得十分普遍。目前中心化交易的低效、高成本会成为星际贸易的强大阻力，区块链技术的去中心化特点恰恰解决了这个问题。

星际链 Interstellar chain

1. 什么是星际链

星际链是基于区块链技术开发的去中心化、低成本、隐私平台，它能够支持星际间大规模贸易的记账，包括未来星际土地的拍卖、转让。

2. ISC (星际币) - 星际链的代币

ISC (星际币) 将作为星际链的代币，缩写为 ISC。目前在星际链 Interstellar chain 上 ISC 所发行代币量为 10 亿枚，未来每出现一个新的人类殖民地或登陆星球则增发 10 亿枚，新增发的星际币将 1：1 赠予先前的持币人。

3. ISC 参数及发行方式

中文名：星际币

英文名：Interstellar chain

英文简称：ISC

发行总量：10 亿枚，未来每出现一个新的人类殖民地或登陆星球则增发 10 亿枚

发布日期：2017 年 11 月 10

发行方式：系统预产生 10 亿枚，团队 2 亿枚，8 亿枚通过相关渠道赠予

4. 关于团队

星际链团队目前近 130 人 (持续扩张中)，总部设在德国汉堡，由 9 年区块链和数字货币开发经验的传奇人物-Aron 博士、金融领域执掌数十亿资本的投资经理人 Jovian、以及

互联网设计“鬼才” Noble 所带领的一众极客组成。

核心团队成员在一起工作配合超过 5 年以上，默契且稳定。星际链团队具有超强的从概念，到策划，到产品设计，到前后端多版本技术快速实现的能力。

5. 星际链的优势

• 公开性

星际链系统的设计公开透明，公开透明性是整个星际链系统的基石。

• 去中心化性

没有中心化个人和组织能控制整个星际链。这条特性决定了自相似性，去中心化特性保证了星际链系统的生命力。

• 安全性

星际链在比特币开发原理的基础上提升了安全机制，在技术上具有超越比特币原理的特征。星际链的创造和转让是基于一种互联网的开源加密协议，不受任何中央机构的管控。

• 价值性

星际链系统必须是具有使用价值的，比如比特币系统的国际支付网络、匿名交易、避税、价值存储、不可冻结、不可监管特性。星际链是基于比特币区块链技术系统上开发的去中心化、低成本、隐私的平台，能够支持星际间大规模贸易的记账，包括未来星际土地的拍卖、转让。

技术部分

1. 共识算法

星际链是一个公有区块链，公有区块链有几种杰出的共识算法设计，包括由比特币系统首创的工作量证明机制 POW (proof of work)，由点点币系统首创的权益证明机制 POS (proof of stake)，由比特股首创的权益代表证明机制 DPOS(delegate proof of stake)，此外还有其他一些拜占庭容错的机制 (BFT，拜占庭容错，Byzantine Fault Tolerance)。

大多数加密货币都选择性忽略拜占庭容错算法，因为这个算法不解决代币分发的的问题。星际链的 ISC 虽然不是货币，但是作为对网络安全有贡献节点的回馈，ISC 将被分发给这些节点。

未来随着项目的成熟度增加，星际链将切换到一种改良的 DPOS 共识算法上，这种算法将考虑“币区块高度销毁”这个重要指标设计。

2. POW 机制

在星际链系统前几年的运行时间中，它将采用一个去中心化的时间戳服务以保障系统安全。我们会避免使用比特币的 SHA256 算法和莱特币的 scrypt 算法，原因是避免比特币或莱特币矿池 51%算力攻击。目前我们计划采用 ETHASH 算法。

3. HBTH-DPOS

虽然 POW 机制可以帮助星际链系统在最初的几年内有系统安全保障，但是 POW 也有自身问题。由比特股首创的 DPOS 权益代表证明机制，相比 POW 和 POS 而言是一个更健壮和去中心化的机制。

不过 DPOS 共识算法的设计仍有两个缺陷：首先是金融干扰问题，攻击者可以通过短期内持有大量系统代币投票支持或反对系统中重要的议案，待操纵完这个投票议案之后再抛售代币，最后从市场上获利。

其次是投票者冷漠问题，选票持有者一般对系统的工作状况并不关心，他们中的大部分人选定自己的代表之后就不愿意再去改变，甚至当代表们作恶的时候也动力不足。

星际链改进了 DPOS 共识机制，加入了币区块高度和心跳的概念，基本模型如下：

币区块高度（TH）源于币天销毁的概念；

比特币的币天=比特币数量×上一次花费至今的天数；

$TH = ISC \text{ 的数量} \times \text{上一次花费至今的区块数} \times \text{星际链常数}$ 。

星际链将 TH 作为 DPoS 中投票的权重，目的是避免金融干扰问题，如果攻击者临时从市场获得大量的 ISC 打算对投票进行影响，那么他们的币区块高度将很小，因此投票的影响力也很弱。攻击者为了达到目的，将不得不从市场上获得更多的 ISC，或者持有 ISC 达到足够长的时间来获取币区块高度，但不论哪一种方式都将显著增加攻击者的成本。

在 DPoS 阶段，星际链与其他采用 PoS 共识机制的系统一样，会根据当时的权益持有情况把 ISC 分发给不同的 ISC 持有人。但不同之处在于，星际链系统的 ISC 持有人将不是以被动接收代币的方式获得新的 ISC，而是需要持有人向系统发送一个“心跳”以证明该 ISC 持有者还是活跃的。同时这个心跳相当于一个来自 ISC 持有人私钥的数字签名，ISC 持有人在发送心跳的时候还要选择更换或维持自己的权益代表。

在 DPoS 阶段，我们也将考虑使用 Power-DPoS 改进算法。

4. 交易类型

为了防止双花，并增加交易的并发性和处理效率。星际链中引入了扩展的、支持多种资

产类型的、一个交易的未花费交易输出 UTXO，它是星际链中的一个交易的基本单位。一旦一个交易使用某一个特定的输出，则其他交易不能使用相同的输出。整个星际链都维护着一个全局的 UTXO 池，所有区块的输入其实都会关联到现有的一个或多个 UTXO，一旦交易得到确认，则这个交易中被使用的输出则被销毁池中移除，新的未经花费的 UTXO 输出则被加入。

星际链的交易类型，大部分采用的是 UTXO 模型。结合星际链的账户系统，改进了传统的 UTXO 模型以提高效率和减少交易大小。

5. 跨链虚拟机

星际链将所有研究力量放在跨链交易的虚拟机的研发上，实现不同公有区块链之间的价值交换。

潜在的风险及考虑

随着区块链技术与行业整体态势的不断发展,星际链可能会面临一些尚未预料到的风险。

请参与者在做出参与决策之前充分了解团队背景、项目整体框架与思路,合理调整自己的愿景,理性参与。

免责声明

1. 本文档仅作为传达信息之用，文档内容仅供参考，不构成在星际链及其相关公司中出售股票或证券的任何投资买卖建议、教唆或邀约。此类邀约必须通过机密备忘录的形式进行，且须符合相关的证券法律和其他法律。

2. 本文档内容不得被解释为强迫参与代币销售。任何与本白皮书相关的行为均不得视为参与代币销售，包括要求获取本白皮书的副本或向他人分享本白皮书。

3. 参与代币销售则代表参与者已达到年龄标准，具备完整的民事行为能力，与星际链签订的合同是真实有效的。所有参与者均为自愿签订合同，并在签订合同之前对星际链进行了清晰必要的了解。

4. 星际链团队将不断进行合理尝试，确保本白皮书中的信息真实准确。开发过程中，平台可能会进行更新，包括但不限于平台机制、代币及其机制、代币分配情况。文档的部分内容可能随着项目的进展在新版白皮书中进行相应调整，团队将通过在网站上发布公告或新版白皮书等方式将更新内容公布于众。请参与者务必及时获取最新版白皮书，并根据更新内容及时调整自己的决策。星际链明确表示，概不承担参与者因依赖本文档内容、本文信息不准确之处及本文导致的任何行为造成的损失。

5. 团队将不遗余力实现文档中所提及的目标，然而基于不可抗力力的存在，团队不能完全做出完成承诺。

6. ISC 作为星际链的官方代币，是平台发生效能的重要工具，并不是一种投资品。拥有 ISC 不代表授予其拥有者对星际链平台的所有权、控制权、决策权。ISC 作为在星际链中使用的加密代币，均不属于以下类别：(a)任何种类的货币；(b)证券；(c)法律实体的股权；(d)股票、债券、票据、认股权证、证书或其他授与任何权利的文书。

7. ISC 的增值与否取决于市场规律以及应用落地后的需求,其可能不具备任何价值,团队不对其增值做出承诺,并对其因价值增减所造成的后果概不负责。

8. 在适用法律允许的最大范围内,对因参与众筹所产生的损害及风险,包括但不限于直接或间接的个人损害、商业盈利的丧失、商业信息的丢失或任何其它经济损失,本团队不承担责任。

9. 星际链平台遵守任何有利于代币销售行业健康发展的监管条例以及行业自律申明等。参与者参与即代表将完全接受并遵守此类检查。同时,参与者披露用以完成此类检查的所有信息必须完整准确。

10. 星际链平台明确向参与者传达了可能的风险,参与者一旦参与代币,代表其已确认理解并认可细则中的各项条款说明,接受本平台的潜在风险并自担后果。

11. 禁止代币销售的国家公民不被允许参与。

结论

与比特股相似，星际链是从比特币系统中受到启发，使用区块链技术来解决未来星际间的土地、能源、矿藏以及知识技术的交易。能够支持星际间大规模贸易的记账包括未来星际土地的拍卖、转让。

在星际链中，通过价值中介起到的作用，智能资产可以在不同数字身份中进行各种安全的转移。得益于区块链技术，星际链天生继承了其不可篡改的账本以及不可双花的优点，星际链将在数字资产和可数字化资产的海洋徜徉。

星际链团队

2017 年 11 月 6 日