ION 技术白皮书

ION 白皮书 v.0.1 地址：
https://github.com/ionomy/ion/wiki/ION-Technical-Whitepaper

这个“动态文件”会被及时更新和修订，直到 ION 正式对外公布。

摘要

ION 是一个基于分布式加密数字货币的区块链，以数字货币奖励网络参与者，通过静态股权证明。ION 奖励“联网时间”而不是“币龄”，因此消除了对交易所和鲜于对网络作贡献的用户的依赖。通过静态奖励制度，参与所得收益与每个活跃节点贡献的工作量是成正比的。这可以防止中心化并促进网络的正常运作。除了静态奖励，ION 还实现了一种主节点网络（masternode network）以激励大股东，并执行高级功能，如附近即时交易和私人交易。

本文会介绍基本的货币描述、特征和功能。此外，本文还会介绍货币的发行、资金用途、未来的发展成果和 ionomy.com 是如何参与到其中的。

ION 的长期战略是，搭建颇具潜力的专注于游戏和数字商品方面的加密数字货币生态系统。

ION的货币技术和ionomy.com的业务规划共同作用，以维持一个积极向上和富有竞争的商业环境。
想要深入了解ionomy.com的商业模式和ION与公司如何协调运作，请阅读ionomy.com的白皮书：
https://ionomy.com/about/whitepaper

目录

货币概述

- **静态股权证明，第 3 版**
- **ION 币初始发行量：10,900,000 个**
    - ✧ 其中，500 万个 ION 币会通过初始货币发行（ICO）与比特币和各种其他加密数字货币进行兑换。
    - ✧ 另外，340 万个 ION 币会被分配到 ionomy.com，作为对玩家的结构性奖励并通过 ionomy.com 所设计的游戏应用来分配。
    - ✧ 还有 250 万个 ION 币保留下来，为货币发展支付赏金。
- **区块奖励**
    - ✧ 第 1 年 = 每个区块 23 个 ION 币

- ✧ 第 2 年 = 每个区块 17 个 ION 币
- ✧ 第 3 年 = 每个区块 11.5 个 ION 币
- ✧ 第 4 年 = 每个区块 5.75 个 ION 币
- ✧ 第 5 ~ 9 年 = 每个区块 1.85 个 ION 币
- ✧ 第 10 ~ 100 年 = 每个区块 0.2 个 ION 币

- **最终货币发行量：总共 5500 万个**
- **区块链特点**
  - ✧ 目标区块生成时间：1 分钟
  - ✧ 区块大小：1 KB 到 8 MB
- **主节点**
  - ✧ 20,000 个 ION 币的交易需要 15 个区块确认
  - ✧ （与普通节点）同等的验证网络正常运行时间
  - ✧ 私人交易（向主节点支付 0.01 个 ION 币的手续费）
  - ✧ 激活主节点可以按比例收取各区块奖励的 50%。
- **股权钱包**
  - ✧ 连接钱包的奖励与网络正常运行时间和货币数量成正比
- **货币发展路线**
  - ✧ 利用特定的奖励雇佣有才华的开发人员以完善货币功能
  - ✧ 当代码被验证满足悬赏规范并被整合到 github 上的 ION 核心代码后，开发人员将得到相应的报酬

工作量证明 vs 静态股权证明

比特币实现了第一个基于区块链的分布式交易账本，同时也是一种不为任何人改变的数字货币。为了实现这一点，比特币对分布的运算设备进行奖励，以维持去中心化的区块链和安全的网络。在很短的时间段内，这种模式的效果很好，但如今比特币奖励的对象是集中的算力，只有少数矿池在维持网络。

比特币网络的迅速增长也对生态环境造成灾难性的负担。算力迅速扩大的同时也导致了运算难度相应地上升，因此挖矿消耗大量的电力。

这种算力集中的情况威胁到了去中心化的验证和平衡模型，甚至其管理权超过了核心开发小组，更何况是要考虑如何解决日益严重的问题。单笔交易确认可以超过 12 分钟（根据 2016 年 blockchain.info 的数据），而且这种技术容易受到攻击而增加延迟。

因此，ionomy.com 不采用挖矿和工作量证明作为安全基础，而是通过股权证明来代替。

对工作量证明的批评促使了股权证明（PoS）的发展并作为替代协议而存在。PoS 系统依靠一个低能耗、分布式的运算网络同样实现了一种安全、去中心化的区块链。它们依靠货币的积聚而不是算力作为保障网络安全的奖励性基础。

早期的股权证明模型是围绕“币龄”和“货币权重”而设计，“币龄”即货币在钱包中持有的时间长度，而“货币权重”即钱包中货币的总量。这些都被证明是奖励的必要而不充分条件，因为它们没有奖励为网络交易提供便利的人。理论上，而且在实际上，基于第一个版本 PoS 的加密数字货币持有人可以存入大量货币于一个钱包，使其离线并积累很长一段时间的币龄，然后在钱包再次联网时瞬间即可获得即时奖励。

第一个版本 PoS 奖励用户持有货币，但没有鼓励他们积极维护网络的诚实性。在这个模型中，货币交易所与其它大股东持有离线的钱包，他们只会定期将钱包联网以生成和出售部分股份。如此降低了货币的市场价值的同时，直接增加了货币发行量。

相比之下，ION 采用“静态”股权证明系统，即第 3 版 PoS（亦称 PoS 3 或 SPoS），它将用户行为结合到奖励条件中，促进用户去积极维护一个强大、快速和安全的网络。奖励是“静态的”，因为它始终是相同的（区块奖励中的 50％）。货币权重依然重要，但“联网时间”（钱包维护活动网络通信的时间）取代了币龄而作为主要的股权概率参数。因此，奖励是根据钱包中 ION 币持有量和积极维护网络安全运行工作而定的。

此外，ION 利用主节点（Duffield，2015 年）来奖励大量持有货币的人，这样有助于网络的健壮性，并且可以实现高级功能，如附近即时交易和私人交易。

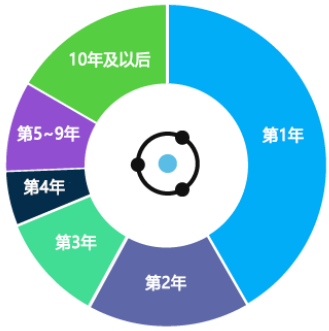
初始货币发行量

总共 10,900,000 个 ION 币将被用于初始货币发行。这批货币由创世块产生，并将由 ionomy.com 信用托管。货币将会按如下分配：

- 500 万 ION 币会通过初始货币发行（ICO）与比特币和各种其他加密数字货币进行兑换。关于 ICO 的详细信息和价格可以在 ionomy.com 中找到。ICO 的过程将由 ionomy.com 管理，而且未售出的货币会用于鼓励独立开发人员将他们的游戏整合到 ionomy.com 中。
- 340 万 ION 币会被分配到 ionomy.com，并将通过 ionomy.com 设计的游戏应用作为结构性奖励而分配给玩家。这些奖励措施是为了将货币分发出去，壮大用户群，并让用户参与到 ION 的社交、金融和游戏经济之中。

- 250 万 ION 币被保留下来，将用作促进货币发展的悬赏支付。赏金有助于分布式发展，通过加密空间邀请跨界精英，带来头脑最优秀的人为 ION 经济（“ionomy”的来源）做出贡献。悬赏还允许社区发布任何所需功能而设的奖励以推动措施。最初的发展重点会在下文*悬赏措施*一节中详述。

区块奖励时间表



年份	每个区块的奖励（ION币数）	每年可获得ION币数	总数
1	23	12,000,000	22,900,000
2	17	9,000,000	31,900,000
3	11.5	6,000,000	37,900,000
4	5.75	3,000,000	40,900,000
5-9	1.85	1,000,000	45,900,000
10-100	0.2	100,000	55,000,000

货币的分配

许多竞争币在开始阶段会实行工作量证明。开发者的理由是，矿工会参与到货币经济中并通过挖矿工作赚取货币。然而，Ionomy.com 团队从加密数字货币的历史中吸取了教训， PoW 阶段鼓励“挖矿和倾销”从一开始就压低了资产价值。简单地使用挖矿这种所谓“吸收”用户的手段，只是为了快速获利然后转身即走，这样无法让货币本身和使用该货币的社群产生持续性的价值。

但是，ionomy.com 的商业规划其目的是，为了维护社区持续使用 ION 币以保持其交易价值，通过局部集中的方式来发展货币的价值。有关该商业模式更全面的详细信息，请参阅 ionomy.com 白皮书。

根据其商业规划，ION 币的分配均使用 ION 技术，并通过 ionomy.com 游戏公司进行。在技术方面，ION 币会根据钱包和主节点所持有 ION 币数量而作为网络安全和区块链维护的奖励而进行分配。在商业方面，ionomy.com 会奖励对 ionomy.com 投资和社交平台的参与者，还会就投资、参与和为 ION 社区做出贡献来奖励游戏平台中的玩家。这种联合分配模式保障了技术基础设施，还可以利用活跃的用户群充实 ION 经济。这个规划的目的是产生持续的 ION 用户流，并使得货币能够保持交易价值。有关该商业模式更全面的详细信息，请参阅 ionomy.com 白皮书。

区块链参数

- 目标区块生成时间：1 分钟

- 区块大小：1 KB 到 8 MB
- 私人交易手续费：0.01 个 ION
- 第 3 版静态股权证明
- 见附录 A 中的 ION 区块例子

一分钟的区块生成时间和最小交易手续费相结合，是在设计时考虑到了交易速度和安全性。充足的区块大小可以在网络交易量增加时放大。总的来说，这些区块链参数是为了防止恶意攻击者以虚假交易堵塞网络，比特币交易在前段时间发生过这种情况并且使得交易变得十分缓慢（Gautham，2016）。恶意攻击者仍然可以尝试通过多笔小额交易来堵塞大区块，但他们会发现他们是在浪费自己的时间和金钱。因为主节点会从他们这种失败的举动中收取大笔手续费。

股权钱包

开发者已经开发出了一般用户使用的 QT 钱包、高级用户使用的 Daemon 钱包。钱包将对所有主流桌面平台进行维护，包括 Windows，Mac 和 Linux。QT 钱包和 Daemon 钱包给与 ION 币持有者完全的控制权，其中包括 ION 币的安全以及发送和接收交易。在线钱包有助于网络安全，通过确认包含有效交易的区块的连续性，确认这些区块是否连接到主区块链上，从而维护了所有 ION 币交易的总账。

- 无最低货币数量要求。（钱包中 ION 币总数必须为非零才能收到股权收益。）

- 钱包股权收益 = 每当发现区块时所得区块奖励的 50％。

股权是有概率性的，而且概率分布是根据钱包地址中的 ION 币数量（货币权重）和持有 ION 币的钱包持续联网的时间（联网时间）。有效的网络连接是指，钱包的联网速度足够高而且连接稳定，足以支持区块链。

旧版本的股权证明需要所谓的检查点。检查点是由开发者签名的集中广播的完整节点，旨在股权被区块树所接受之前帮助验证货币股权。在 ION 中，每个节点都是完整节点，因为它不需要检查点系统。通过去除以前的 PoS 版本中存在的这种局部中心化依赖，所有节点都被充分授权，使得网络攻击更加困难。

主节点

保障公开和私人交易

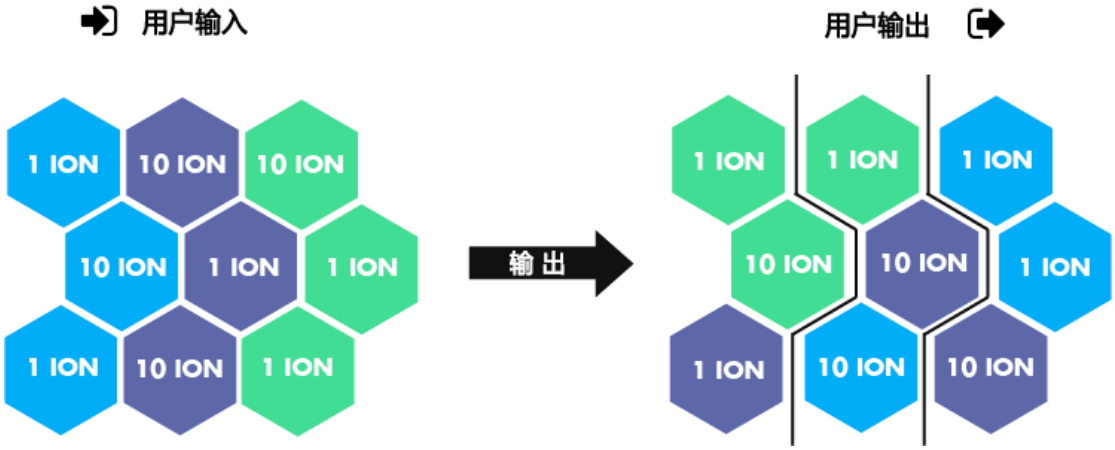
主节点（Masternodes）在约 4 秒内确认所有的公开交易，通过连接网络上所有节点中的每笔交易以避免双花（Duffield，Schinzel 和 Gutierrez，2014 年）。当私人交易被启动，主节点也会执行必要工作让交易难以被追查。主节点还可以执行附加功能，例如新的发展被委托和悬赏被实行。

主节点参数

- 最小及最大货币数量要求均为 20,000 个
- 奖励：50%的区块奖励 + 该区块中包含的所有交易手续费
- （与普通节点）同等的验证网络正常运行时间

私人交易

主节点通过一种分布式混合服务促进私人交易，该服务拥有完美的货币可替代性的优势。任意单位的 ION 币与任何相同大小的其它单位的 ION 币都具有同等价值，无论其交易记录如何。主节点利用这一性质，自动将私人交易分解成多个相同且不可区分的小交易，既增加了原始交易的复杂性，又混淆了任一单位交易的出处。



***每种颜色代表一个用户的交易*

图2：在这个交易区块的例子中，三个用户设定了各种面额来提交资金。 *即时用户只是向自己支付，新输出的形式也会是随机排列的。 *

ION 币私人交易的发起是通过本地钱包，而接收是通过主节点的子网。交易以三笔为一组被处理。常见的面额输入是必需的——例如 0.1 个 ION 币，1 个 ION 币，10 个 ION，或 100 个 ION 币。

当交易被应用到混合池中之后，接收到的主节点会将交易设置传输到整个网络。如果只有一笔或两笔私人交易被挂单，这些交易将处于排队的状态直到第三笔交易进入混合池。手续费是从每笔交易中收取的，然后总的账目会进一步混淆交易记录。

私人发送被限制到 20,000 个 ION 币，因此大笔交易需要多个会话来彻底脱钩相关的交易记录。由于每个会话被限制为 3 个客户端参与，追踪者有三分之一的机会能够追踪一笔交易。

混合式交易是通过多个主节点链接到一起，使得每增加一笔别的交易，可追溯难度就会呈指数增长。用户对混合程度有一定的控制能力。混合得越多则需要越多的时间，但输入也能混淆得更彻底。这些交易的手续费随混合程度增大，因为这个过程中有越多的主节点参与进来（Duffield 和 Diaz，2015 年）。

这个混合的方法是一种无需信任、集中、链上和网络上的服务，效率高、有效而且安全。它在本地钱包中直接启动，而且无需离开 ION 网络就可以完成。虽然私人交易的一些细节被遮蔽了，但是系统仍然在 ION 区块链上保留了足够供验证的货币花费情况。

运行主节点的动机是什么？

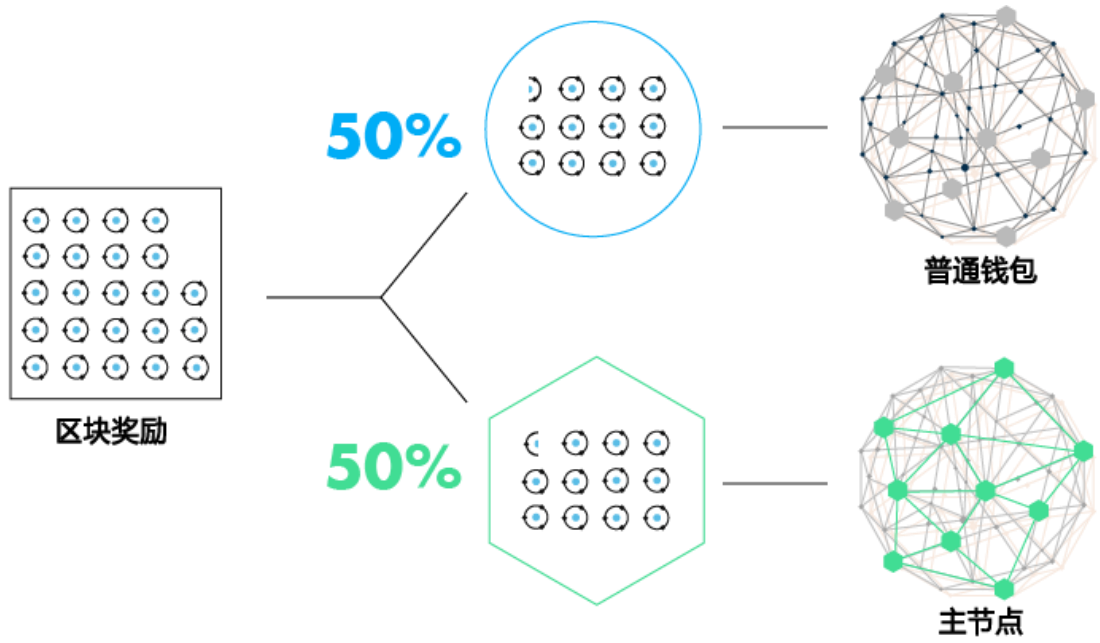


*图 3：平均每日奖励≃（每天发现区块数中的# 个 * 区块奖励 * 50%）/（主节点中的# 个）*

主节点获得固定奖励（50%的区块奖励），奖励在同样参与验证的主节点当中按概率分配。主节点重复地扫描等价节点的性能，只有具有持续、稳定和高联网速度的高性能节点有资格获得奖励。除了获得区块奖励的 50%，主节点还能获得在这个区块中完成的公开交易和发起的所有私人交易池的手续费。这些激励措施促进用户持续联网以维护高性能的网络。

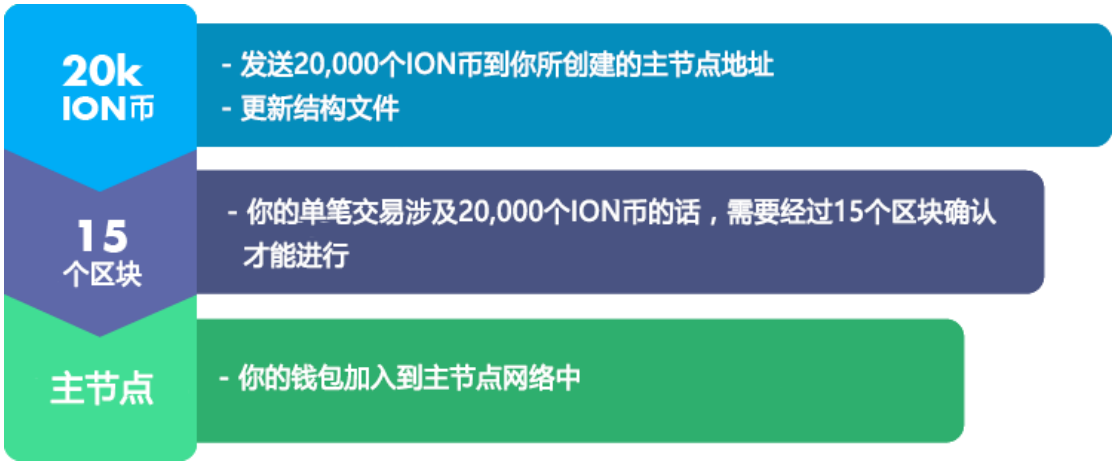


图4：激活主节点所需程序。

主节点网络性能维护

理论上，恶意行为者也可以运行 ION 主节点，但并不提供任何网络所需的有质量的服务。为了减少这种可能性，和让利用该系统获取个人利益望而却步，所有节点都必须定期测试其余的 ION 主节点网络连通性（ping）以确保这些主节点仍保持活动。这项工作是通过每个区块选择 2 个仲裁（quorums）来完成。在每个新区块的哈希（hash）时，仲裁 A 检查仲裁 B 的服务。仲裁 A 是与当前散列距离最近的节点，与此同时仲裁 B 是距离所说哈希最远的节点。

主节点 A（1）检查主节点 B（排名 2300）

主节点 A（2）检查主节点 B（排名 2299）

主节点 A（3）检查主节点 B（排名 2298）

主节点网络是自监测的。每当有新区块添加到区块链时，网络中大约 1％的主节点将被检查。此结果每天在整个主节点网络中被检查大约六次。为了维护这种无需信任的系统，节点通过仲裁系统随机选择；网络也需要至少 6 次违法行为才会停用节点（Duffield 和 Diaz，2015 年）。

货币发展路线

ionomy.com 将通过定义目标，发表悬赏详述，并奖励独立开发者完成和实施委托，以此来促进对 ION 开源核心代码的开发。这种方法允许 ionomy 核心开发团队专注于他们最擅长的事情上，制作 ION 经济核心的移动端及社交游戏。赏金用于从开发者社区中聘请最优秀的人才，以提升核心货币代码，同时使货币的发展去中心化。ION 社区可以合力影响货币的发展方向：如果社区希望实现某种特点，并准备发布一个悬赏，赏金将激励开发者们去完成委托。

赏金款项将被置于多重签名钱包中。赏金发放请求首先会在测试网络环境中生效。一旦认为符合悬赏规定的要求和规范，赏金发放请求将会被合并到 GitHub 上的 ION 源代码的主要分支中，而且赏金会直接支付给代码开发者。

悬赏机制

下面的悬赏已被认定为上市后的重点项目：

- 延时交易/安全地址（在下面的示例＃1 中进一步详述）
- 智能合同/中介
- 彩色币/侧链/资产（见下面的示例＃2）
- HTML5 钱包
- Electrum 钱包
- 基于 java 系统的手机钱包 ION-j
- 钱包内的社交整合

悬赏示例＃1：具有安全地址的延时交易业务*

*问题：*冷钱包——持有货币而又从不联网、完全私下生成密钥的储存地址——是已知的加密数字货币中最安全的办法。用户可以在纸钱包上打印私钥，钱包可以保存在安全的位置。但是，最好的网络取决于在线钱包持有 ION 币的用户的广泛参与。考虑一下这种情况：如果用户 Jane 在工作时让钱包（或主节点）联网，晚上离开时仍保持运行，然后 IT 部门的员工 Dick 可以入侵到她的电脑并且将她所有的货币发送到自己的地址。那么 Jane 将没有任何补救方法。

*悬赏：*创造一个可以保护 ION 币持有者的能够延时交易的安全的地址系统，即使私钥的安全性受到了威胁。开发者将创建一种链上的参数，在给定地址的任意发送动作前设置一个可变的延迟，并且在触发后将钱包内容指向选定的故障地址。现在，如果 Jane 将时间延迟参数设置为 10,000 个区块，那么当 Dick 入侵到她的钱包时，Jane 仍然有一周时间来触发失效保护。如果她没有触发失效保护，Dick 会得到她的货币。但是，如果她能及时知道黑客攻击，就可以简单地发送一个信号，将货币转移到她的冷钱包地址。从冷钱包处，她可以删除泄漏的密钥，并采取新的安全措施和获得新的密钥，访问她的安全钱包并重新开始股权收益。完成悬赏的开发者将为 ION 用户提供一种全新水平的安全保障：“暖”钱包，打破冷钱包的安全性和热钱包的实用性之间的平衡。“股权安全”系统将会优化网络的速度和安全性并促进大众参与使用。

**此悬赏示例是为了说明情况的一个简化。在 github 上发布的实际的悬赏，将全面详述具体要求和参数。*

在上下文中所说的货币

从历史上看，大多数加密数字货币旨在激励矿工和股东去发展和保护网络。由于低难度的挖矿有着高利润，这为货币带来了一些关注并开始分发货币。但是，这些用户很快就放弃了他们所持有的没有持续的价值驱动力的货币。正因为货币发行量的增长比需求量要快，供过于求，降低了货币的价值。尽管货币可能现在稍微更加分散了，但它们仍然集中于核心用户和短期持有者构成的群体内，他们的主要兴趣是经济利益。投机者和贸易者可以购买货币，但他们也还是短期持有者。价格操纵和大量抛售的循环重复，结果是随着时间的推移，货币由于乏人问津而贬值和信誉不佳，而且由短期牟利者构成的用户群也没有对长期投资的兴趣。

相反，ionomy.com 和 ION 之间关系被设计成开始时的价值创造者。ionomy.com 制作和销售数字商品，重点放在移动端和社交游戏应用上。公司为社交和财政奖励系统提供资金，以培养接合的用户群。活跃于公司的产品范围内的用户将会获得奖励。通过不断为 ION 创造优秀的用途，公司激励更多的用户加入到生态系统之中。然后，用户群会消耗更多 ION 币，创造出需求量和稀缺性。

与此同时，主节点奖励用户以持有 ION 币并为保护网络和区块链完整性而努力。此外，ION 拥有强大的技术能力，旨在吸引企业家建立新企业、扩大用户群并增加货币的效用。

结论

ION 将主节点/钱包系统整合到静态股权证明（第 3 版 PoS）中。其结果是实现快速的交易确认、可靠的网络安全性，通过分布式货币混合增强私密性，并且可以减少价格波动。此技术基础确立了智能合同、彩色币、侧链和高级安全机制实现的可能性。

ION 强大的货币技术与 ionomy.com 创新的企业计划的这种组合带来了引人注目的机会。企业家和开发人员可以利用社交网络来吸引客户和投资者，这是该行业中从未被人尝试的方式。

致谢

特别感谢的特约编辑包括：

Robert Hoppenfeld，Derek Broyhill 和 James Pass

参考文献：

Blockchain.info. (2012). *Bitcoin Median Transaction Confirmation Time (With Fee Only)*. Retrieved from https://blockchain.info/fr/charts/avg-confirmation-time

Duffield, E. (2015). *Dash: Video Series - #4 - Incentivized Infrastructure and Masternodes. *DVS15E04. Retrieved March 28, 2016, from https://www.youtube.com/watch?v=FY1mciGGhO4.

Duffield, E. and Diaz, D. (2015). *Dash: A Privacy-Centric Crypto-Currency*. Retrieved from: https://www.dash.org/wp-content/uploads/2015/04/Dash-WhitepaperV1.pdf.

Duffield, E., Schinzel, H., and Gutierrez, F. (2014). *Transaction locking and masternode consensus: A mechanism for mitigating double spending attacks*. Version 2. Retrieved from https://www.dash.org/wp-content/uploads/2014/09/InstantTX.pdf

Gautham. (2016). *Blockchain Monday Blues Due to Spam Transactions on Bitcoin Network*. NEWSBTC. Retrieved from: http://www.newsbtc.com/2016/03/02/bitcoin-network-spam-attack/

附录 A

ION 区块实例

```
SetBestChain: new
best=0254614e1a37e7d1681738031a1ea18efa53773972b1b6cedeafb1a4877d926c
height=5043
trust=23477951177320352418
blocktrust=1099304894429909
date=04/05/16 21:52:00
ProcessBlock: ACCEPTED
connected to self at 25.12.221.127:39286,
Successfully synced, asking for Masternode ist and payment list
IONd masternode list
{
"25.12.221.127:9999" : 0
}
CommitTransaction:
CTransaction(hash=fff53d85c32a301bf61d6cde7951667e7740292e8f360c614aeb18eed
7a143e8,
```

```
nTime=1459893428,
ver=1,
vin.size=1,
vout.size=2,
nLockTime=0)
CTxIn(COutPoint(50f90a5bc8, 1),
scriptSig=3045022100e135cbb17ee9fc)
CTxOut(nValue=1000.00,
scriptPubKey=OP_DUP OP_HASH160 dd28713d7c72c6a6017a98dd8f29743cf4ce6a49
OP_EQUALVERIFY OP_CHECKSIG)
CTxOut(nValue=8.03999,
scriptPubKey=OP_DUP OP_HASH160 7b9a6410aea5fd21755d42778b65b5db5c898b36
OP_EQUALVERIFY OP_CHECKSIG)
keypool keep 13
```