
# APPLICATION BASED BLOCKCHAIN

WHITEPAPER

# 1.使命声明

我们的终极目标是提供一个安全、快捷和用户友好的区块链生态系统，以促进全世界对去中心化服务的实际应用。

# 引言

自从 2009 年比特币网络兴起以来，无数的开发者从事创造具有竞争性的点对点数字货币、资产。这里面绝大部分都是对比特币的简单复制后改个名字，在目的、设计或者功能上几乎没有差别。另一些人则试图改进中本聪在白皮书中提出的“比特币：一种点对点电子现金系统”的路线。从那以后，关于改进这项技术的主要的和可能的建议已经涌现。比特币通过挖矿获得新币对电力需求的持续攀升是一些人希望解决的问题。2013 年 4 月，全球供比特币挖矿消耗的电力估计是每天 150000 美元。到了 2018 年 1 月，全球被挖矿消耗的电力估计是每天 5287349 美元。试图改善比特币挖矿对电力消耗过高的问题，Scott Nadal 和 Sunny King 在 2012 年发表了“点点币：基于权益证明的点对点加密货币”的白皮书。

这使得点点币成为一个只需大约 30%的比特币耗电量的加密货币，白皮书还介绍了其他一些改善，例如降低了被矿工垄断的风险和发生 51%攻击的可能性。基于权益证明的铸币使得形成垄断的成本更高昂，并且分散了基于工作量证明的挖矿奖励被垄断的风险。随着这些及其他区块链技术的改进，I/O digital 团队在创建者 Joel Bosh 的领导下设计了与众不同的 POS 方法，并在 2014 年 7 月 23 挖出了 IOC 的创世块。I/O Digital 开发团队发起

I/O Coin (IOC) 时没有任何的 ICO 和预挖，通过挖矿公平启动。为确保公平和均衡分布，在切换到基于权益证明(PoS I/O)之前，团队在基于工作量证明(POW)的 X11 算法原

码中添加了一个复杂的密码哈希。I/O Digital 团队从那时起就专注于为具备安全的、全球可采用的和可扩展性的 IOC 区块链添加进一步改善和用户友好的功能。

# 2. I/O Digital 区块链现状

IOC 最初公平发起的重要性，使其有一个健康成长的时期，同时通过功能、支持和信任实现协同效应。IOC 区块链在超过 32000 小时的 POS 计算中 100%保持正常运行状态，未曾出现过接近 51%攻击的情况，从创世块开始，IOC 社区就维持超过 46%的币在 staking。这是维护区块链安全的强健承诺。社区就更新问题已取得了 100%的共识，并且公共节点在全球超过 65 个国家被激活。IOC 近来在 2016 年赢得了区块链类别的欧洲 Fintech 大奖，Benzinga Fintech 大奖，并且是 2016 年欧洲 Fintech 大奖中参加决赛的选手。
IO Digital 开发团队的目标是创造一个安全的，改变现有规则的，用户体验友好的区块链框架，团队的激情和决心驱动我们专注于我们的目标，我们一直以来把开发放在第一位。基于这些原因，团队成立了官方的非营利基金，用于将来对 I/O Digital 公链应用的教育。这些是为了提高公司、个人的认知度，以获得对基于服务的 IOC 区块链应用的实际应用。

# 3. 问题描述

跟随中本聪的脚步，IOC 已经挖出了一千六百万币，后续通过 POS 奖励机制，在 2052 年的时候将达到二千二百万的总量。成功交付我们的初始版路线图后，开发团队便着手了第二个区块链更新工作 DIONS（去中心化的输入/输出名称服务器）。DIONS 支持把文档和身份数据存储在区块链上，还允许在一个完全别名系统里使用 AES256 算法对信息进行加密。IOC 数据存储、信息发送/别名系统等产生的费用被重新分配给网络上的活跃 stake 者，这确保了未来 IOC 的分配并且激励用户参与 stake 维护网络安全。

考虑到数据膨胀、安全漏洞和用户功能不友好等风险，开发团队意识到单链将成为过去式只是一个时间问题。团队部署了一个具有积极目标的路线图，并且快速地计划将其升级到 IOC 的主链上，代号 DIONS。升级的重点是实现作为团队计划的变色龙侧链的一个入口注册商，为了使这些成为可能，平台的核心算法升级至一个新的权益证明算法，代码为“CiPher”。

我们通过 staking 和安全增强、去中心化加密数据、信息和新的别名系统，与“CiPher”一起加强了平台的健壮。随着所有这些功能与我们分散式的类 GPG 系统一起部署，DIONS 将被证明能够成功地将这三个主要组件结合起来，实现真正用户友好和先进的区块链平台。维护 IOC 区块链安全的 stake 者将获得每年%4 比例的 staking 奖励，此外还有交易和注册别名所产生的费用被重新分配的奖励。

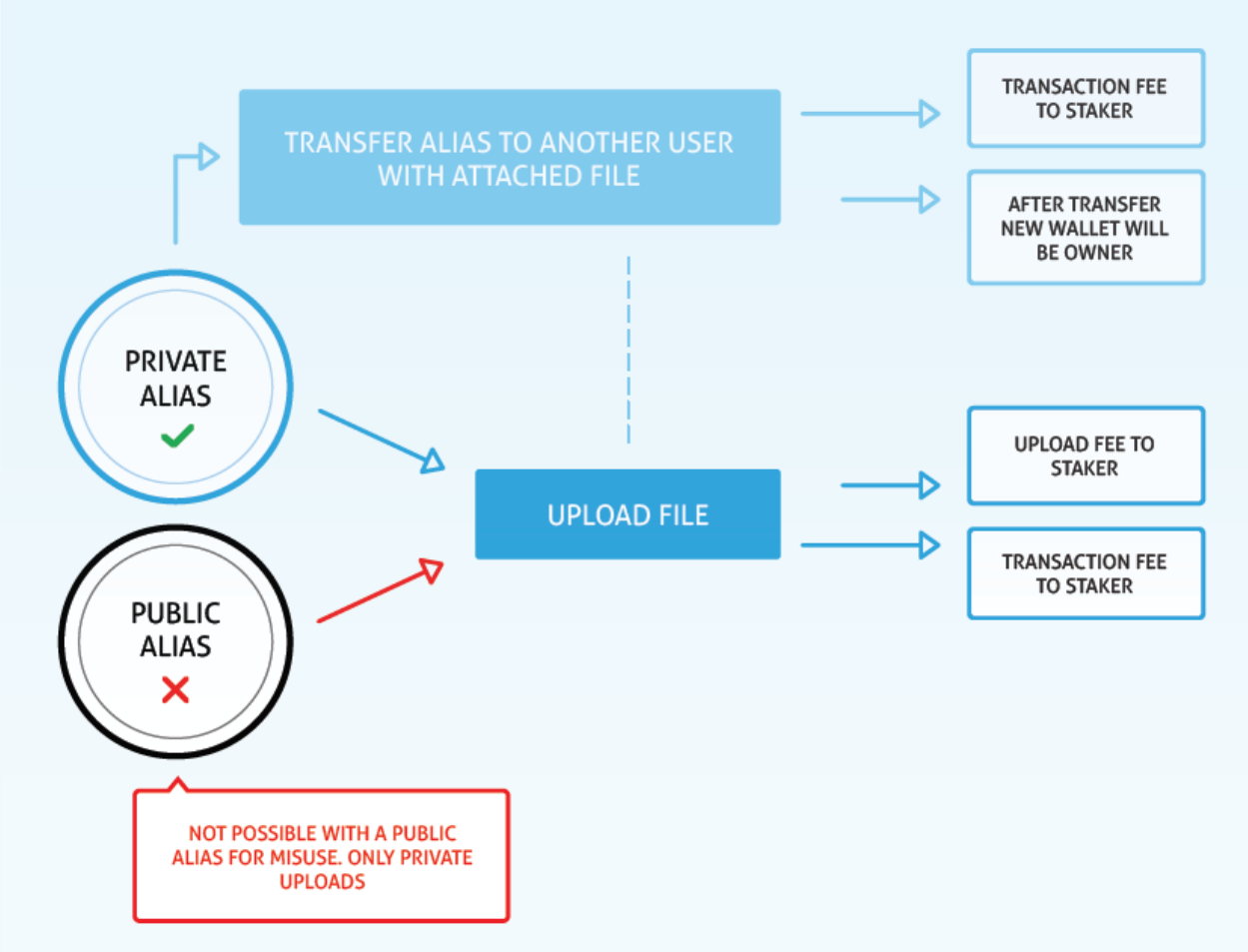
# 4. IOC-DIONS（去中心化的 DNS）

别名键值对为 IP 网络节点的命名提供了一种间接方式，可以认为是为基于区块链的 DNS(域名解析服务器)提供了基础。DIONS 是别名，并提供一个人类可读的名称，可被区块链直接解析。别名可以唯一地归于一个普通的 IOC 地址。DIONS 提供一种把名字映射到位于因特网或私有网络上的资源的方法，这些能够从区块链中直接解决。

# 5. 私有&公开别名

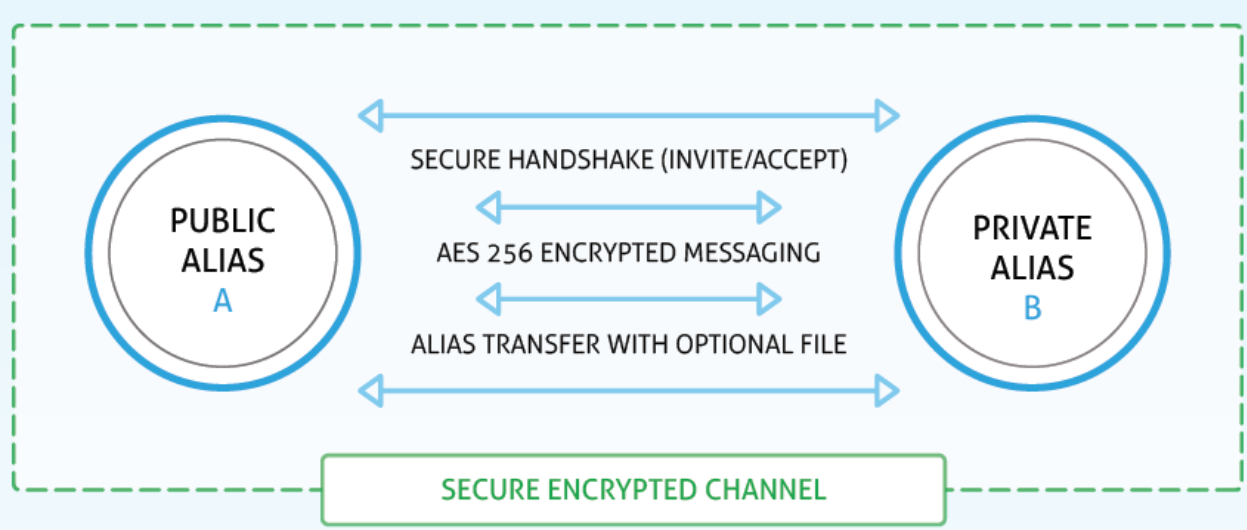
有 2 种类型的别名：公开(不加密)和私有(加密)。一个别名是 IOC 十六进制地址标识，最多可有 255 个字符的纯文本密钥。在任何给定时间，一个别名都会准确地标识为一个 IOC 地址。私有别名为私人所用。别名一旦被创建，产生键值对将被加密，成为私有，在区块链上不可见，这将缓解别名占用。私有别名在用户注册中保持私密，并且一个加密状态的别名不能接收 IOC。用户只能使用私有 DIONS 来进行文件存储和安全的文件传输。别名一旦被创建，用户可以用它配对一个特定文件或者将它在应用程序区块链中转移给其他用户。

数据的传输通过构建一个信道实现，加密别名将为接收方加密所有相关数据。因此，净负载数据量(和传输量)可能会因为双重加密处理而变化。
为了接收 IOC，私有别名可以通过简单的解密变为公开别名，别名一旦变为公开，别名就附加到一个公开地址上并能够接收 IOC。随后，在大约 25 万区块到期间隔后所有别名将失效，在此过程不发生更新。




# 6. 私有别名转让

私有别名可以转让。用户为了发送或者接收别名，用户必须从一个公开别名(A)中发送邀请给公开别名(B)作为 RSA 密钥交换，这将初始化一个加密通道，使其具有传输别名的能力，但同时也初始化用户间的信息通道。如上所述，我们在通过别名关联的两端建立了一个信道，在这种情况下传输的别名是使用私钥进行加密的，如果是其他的需要传输的负载则使用对称密钥加密。




# 7. AES 256 加密信息

一个信道在 2 个公开别名间建立起来后，即可进行点对点的加密信息发送和接收。与一个 ssh 会话的协商类似，信道的首次协商是使用 RSA 加密算法，之后所有的传输负载加密都使用更高效率的对称密钥完成。在 RSA 交换对称密钥之后，用户可以马上在加密的通信信道中进行交流，无需进行信息发送确认，因此可以即时进行。信息的加密依赖于 AES 256 位密钥，每个通道一个，每个消息 128 位初始化向量。

# 8. 数据存储

如前所述，利用 DIONS 可选择存储加密内容，内容是经 base64 编码过的，其源数据可以是（例如）ASCII、PDF、JPEG 或任何二进制数据。当前每一个 DION 别名可选择上传的容量限定在 1MB。用户的加密文件上传成功后，他可以将它发送给另一方，为此，二者将建立一条加密信道并且传输的数据使用 AES256 位进行加密。数据被用户上传和加密后，该用户就可以永久地对其进行下载和解密操作。因此，加密的数据可以是私有的，不管它是否用于信道或共享加密传输上。

# 9. POS CiPher

这是一个维护区块链安全的过程。随着近来对前述内容的实现和启动，同时也对 staking 机制进行反思。自 2017 年 11 月起，币龄参数从 staking 的算法模型中移除。新的挖矿模型确保符合追求 staking 奖励最大化而长期运行节点的 stake 者的最佳利益。

# 10. 币龄&洗牌

现已不再有延迟奖励的任何概念。只有链接起来并且竞争出块的节点才能获得奖励。我们还采取对 stake 地址重新洗牌的进一步措施来防止 staking 奖励倾向有利于持有更多币的地址，这项措施显示了它在平衡地址间分配奖励的运作是有效的。

如果一个钱包里有 IOC，它可以马上开始 stake 和接收奖励，只有当钱包处于运行中并且 staking 模式下才能接收奖励，奖励是每个块固定的 1.5 IOC 加上包含 DIONS 交易费在内的任何交易费用，将来奖励和费用调整将在每个治理共识的间隔更新至代码中(截止本文编写时，DIONS 的费用是 0.01 IOC 加上每千字节数据 0.01 IOC）。

# 11. 信道&原子键

一个信道通过将两端与一对称加密密钥关联建立起来。信道是数据存储和通信基础设施的核心。双向信道的建立涉及到对另一个别名目标发起邀请，如果对方接受邀请，则建立必要的密钥交换以支持加密通信和加密数据的传输。目前，所有的加密私钥都保存在 wallet.dat 里。为支持备份和对存储于不同位置的私密密钥管理，在第一至第二季度间将会提供一个并行的 API 选项。

# 12. BIP65

在 2017 年 11 月发布之前，我们开始了对 bip65 的实施。这样做的目的是允许事务输出在锁定阈值（可以是块高度或块时间）下进行检查。这样可以锁定相应的输出，直到达到指定的时间阈值。

# 13. 隐身地址

第二季度隐身地址功能将会被添加到系统中。隐身地址是保护私有数据和 ioc 接受者的方便方法。例如，医疗记录被无痕上传和传输，或者一个供应商将他的付款地址放在网站上或其他公开场所,但对销售商来说把收钱的地址显示给所有人看可能会是个问题。隐身地址在这些场景下可以保护隐私,它使付款方基于一个单一的公共隐身地址生成一个一次性付款地址。

对于一个给定的隐身地址(P, Q),通过使用一个实质上非常大的随机数 r 产生的乘积 "r.G=R"来生成一次性地址。实际上，"r.P = r.p.G = p.R"是付款方可以产生一次性地址以及收款方可以独立地、无需依赖任何第三方就能可靠地知道该一次性地址是否为他所有的原因。隐身地址增加的公开组件 Q 以确保只有接收者才能花费发往这个地址的任何资金。因此，我们把 p 叫做隐身地址的内部组件，而 Q 是隐身公开地址(P,Q)的外部组件。

# 14. 环签名

环签名(由 Rivest, Shamir & Tauman 在 2001 年首次提出)计划在第二季度与隐身地址一起实现，它允许在任何公有密钥集生成一个签名，这样生成的签名是不能被判断是使用哪一个密钥来构造的。环签名在实际应用中的一个受限是环签名在许多算法中增长的方式基本上与密钥的数量成线性关系,然而，近来已经提出了包括次线性和恒定大小增长的算法。

环签名可以被看作是隐身地址的组成部分，用户可以用它对交易签名，而任何监测者不能通过环签名交易确定是谁签名。因此，这样的系统将成为 ioc 和文档完全匿名传输的力量源泉。

# 15. 投票

我们的安全信道机制使秘密投票成为可能。任何人对任何事都可进行投票，从潜在的新项目和对等网络网络方向到与私人团体的相关事宜。投票可以通过建立我们所说的投票箱别名进行，这可以是功能性别名或指定的群组。

# 16. 群组加密信息信道

当前系统提供点对点加密通讯，在此方向上后续重要一步是把该功能扩展到群组成员间。最近的事件相关的一些知名加密群组信息平台已经再次证明，开发更多更好的替代方案为

人们讨论政治和技术观点是非常重要的，例如不用担心被封杀、压制或者未经授权而向州政府或独裁政权披露信息。

向加密讨论群组扩展，对于我们的已完全可操作的点对点信息加密网络来说是一个自然、合乎逻辑的过程，这个实现将包含通过对指定别名邀请处理时我们信道协商的自然一般化。作为一个群组，很自然地它属于一个拥有者，并且这个拥有者可以将它转让给其他人。

当成员被接受后，通过一个单一对称密钥建立的多会话允许组成员依次访问群组的所有信息。建立在当前 IOCoin 的 AES256 位信息系统的扩展将为群组讨论提供一种完全去中心化的安全方法，此外，我们还将为一次性信息视图添加相调制解密。

# 17. 科学计算

在我们当前调查中的一个感兴趣领域是通过利用 IOC staking 节点的空闲计算周期来帮助人们提高对癌症发展的认识和可能的治疗方案，其中特别感兴趣的是癌症中有显著分布变化或者变异的蛋白质。研究这些结构需要 x 射线晶体学，蛋白质必须首先进行结晶。这是一个非常复杂的过程涉及许多不同的参数和组合，例如溶液的种类、酸度、温度、疏水性、等电点等成千上万种可能的情况。此外，不同的蛋白质有不同的参数，通过分析数百万次结晶实验得到的数据集，可以确定有效的结晶方法。（不仅对于所讨论的蛋白质，而且对于具有相似结构的蛋白质）。

# 18. 分级 staking

随着对网络安全的愿望的提高，还需要对哪些长期坚持高水平 staking 贡献的节点进行识别。通过增加针对这些节点 stake 的行为特征的奖励来鼓励其他 stake 者参与进来 staking，进而使整个网络受益。强化忠实矿工的利益将涉及到 staking 分级，这将涉及提高网络上的别名和通信相关费用的增长政策，利用这些费用来奖励哨兵节点。潜在的奖励将涉及以某种分级方式再次授予的块投票权。如前所述，投票已经是我们具备的一项功能。我们预期某些类型的投票将以协商一致方式保留，这可能更适合于公共和普选领域。分级 staking 奖励有着明显的优势并且有益于整个网络，该方案目前正在测试中，将在第三或第四季度进行详细介绍及提供完全的文档说明。

# 19. Gettxout

Gettxout 当前正在编码实现，期望第一季度可以完成。Gettxout 在一个给定输出中返回的信息包括块哈希、确认个数和值。Gettxout 功能的实现还将使 IOC 被添加到利用去中心化交易原理的交易平台。

# 20. 变色龙

我们已经研究和原型测试一种机制，它允许使用不同协议和 API 规范的异构网络实体透明地交互操作而不需中央配置。我们所称的连接补丁被开发出来，允许在不同的点对点网络中直接发布交易信息，而只需使用最少的 API 进行集成。

在实际中，我们对 2 个不同的网络中以及连接补丁一起进行测试。交易被发布到连接补丁里的一个地址，与之配对的地址来自另一个网络，通过连接补丁的实现资金转换，因此，这种服务对不同网络的每个用户都是可用的。再次说明，测试是针对 2 个异构点对点网络中进行，但通过使用网络适配 API，可以在更多的网络中实现。

我们研究了连接补丁在进一步服务中的潜力，例如在可以处理面向更多数据的网络，这将提供一个服务专业化和互操作性的有效范例，以及在连接层本身的政策投票。这一结果的第一结果使我们研究提炼和发展最初作为概念验证的东西，结果就变成了变色龙项目，该项目目前正在开发中，并计划在今年晚些时候首次发布。

# 21. 如何使用这些功能

我们开发了一个包含了前面章节所述特性的全功能、透明易用的基于 HTML5 的电子钱包系统。所有特性，包括创建与解密、加密文件作为上传负载和加密文件内容的解密下载-通过个体用户邀请的安全信道协商-接受按钮序列-安全文件传输-安全的即时消息通信。所有这些都在简单易用的 HTML5 图形界面中变得透明。

这样，我们的界面层可以认为是对我们通过 API 接口提供的现有全系列特性的一个标准实现。商业公司、政府部门和机构单位可以使用 I/O Digital 的 API 来定制自己的用户界面，以符合自身领域、自身使用场景以及自身喜爱的外观和感受。
除明确指出外，前述的所有功能在我们的范例软件中都可访问。

# 22. 引用

*[1] "How to leak a secret", Rivest, Shamir, Tauman, ASIACRYPT 2001. Volume 2248 of Lecture Notes in Computer Science, pages 552–565.*

https://link.springer.com/chapter/10.1007%2F3-540-45682-1_32

*Author: Derek Hatton, Joel Bosh*
*January 09, 2018*
*Document revision 1.0*

**I/O DIGITAL Foundation**
www.iocoin.io / www.iodigital.io

**Latest Github developments**
https://github.com/IOCoin/DIONS/releases

Translation by community member "Alberich Power" – thank you