Zen 白皮书

作者：

Robert Viglione, Rolf Versluis, Jane Lippencott*

2017 年 5 月

摘要

Zen 是一个采用零知识技术的端到端加密系统，为通信、数据和价值的传输与储存提供了严密的安全保障。结合革命性的技术，Zen 将传统意义上独立运作的三项功能融合在了一起，它们分别是：交易、通信和竞争性治理，以此加速创新化。借助于可跨越全球分布的区块链技术和计算基础架构技术，此创新过程得以安全、匿名的方式进行。该系统集成了多项一流技术，为不受权限禁锢且可以灵活适应用户偏好的创新发展提供了一个开放的平台。

---

*作者们的联系邮箱分别是：rob@zensystem.io, rolf@zensystem.io, jane@zensystem.io, 在此，十分感谢 Jake Tarren 提出的宝贵意见，同样感谢 Zclassic 和 Zen 社区给予的帮助，最终的成果离不开大家的支持

目录

1. 目标

“在不断的创造中批判。” —— 米开朗基罗•博那罗蒂

我们所生活的世界受到了高度的控制与监视，数以十亿计的人被剥夺了基本的人权：财产所有权、隐私、自由联想的空间和获取信息的渠道等等。我们现有的科技就是用来解决这些问题，而 Zen 早期的任务便是如此。

基于一套核心理念，Zen 运用零知识证明技术，围绕一系列革新性技术建立起集产品、服务与业务于一身的平台。作为一个分布式的区块链系统，加入了最新的抗审查技术、完全加密通信技术和持久的生态治理模式理念，Zen 致力于维护用户的隐私权，提供必需的网络基础架构，使用户在跨国界的生态环境里可以安全地进行合作、创造价值。我们的任务是将一套去中心的，温和并具有自发性的社会结构与后中本聪时代的最新科技结合在一起，提高所有自愿参与者的生活质量。我们坚信这样的理念正是这个时代所需要的。

Zen 是一个安全的、以隐私为导向的基础架构，其集成的治理系统使参与者可以协同在多种维度上扩展功能。例如我们有可能实现：存储个体识别的数据资料、对财产所有权进行选择性验证、金融服务去中心化，实现保护隐私的 p2p 或 b2b 资产置换、互助社团、“点对点”保险、去中心化人道主义援助机制、或者纯粹的仅作为匿名价值代币。

那些由于缺乏身份识别、资金和安全渠道而在银行业务和医疗保健服务上被降低服务级别的人群可以用上这些功能。拥有所有权并希望将个人数据变现的个人也可以利用这些服务。例如，可能有一些创业者希望建立起在小圈子内太阳能的竞标招标制度。有许许多多这样独特的应用，他们基于一个共同的信念：去中心化是道德进步的原动力，自愿的解决方案是最具创意和持久的。

2. 历史

Zen 通过吸收现有的和新的特性，在最佳的加密货币、网络架构、分布式文件共享系统的基础上，为长期的可行性打下坚实的基础。不仅在技术上如此，同样重要的是我们是基于分布式共识和竞争性治理的最新思想。本项目的部分基础来自比特币、Dash、Decred 和 Seasteading。

Zcash 扩展了比特币，加入了完全匿名的屏蔽交易，使用户可以在正常的比特币式地址（T 地址）和抗流量分析的私有地址（Z 地址）之间选择。我们因此创造了 Zcash 的复制品——

Zclassic。我们改变了一些我们认为不重要的主要参数：除去了 20%的创始人奖励并解决了货币发行的慢启动。自 Zclassic 的推出后，我们形成了一个充满活力的开源社区，渴望将技术引向一个独特的发展方向。一些早期的工作包括：为 Zcash 和 Zclassic 开发了一个开源的采矿池应用程序；开发了 Windows 和 Mac 钱包。

我们的团队意识到，在完全加密的网络之上,Zclassic 可以进一步成为一个带有创新的经济和治理模式的网络，这样会更符合中本聪对一个去中心化的全球社区的愿景。在该目标下，我们把 Zclassic 视为是一个纯开源的、全自愿的加密货币项目，Zen 则被扩展成了一个在经济上可以自给的平台，以便于更好的支持更广泛的通信、文档共享和经济活动。

3. 执行细则

Zen 是 ZenCash 代币发行的首要系统，类似于以太坊之于其代币 ETH。ZenCash 为 Zclassic 的一个分叉，并将附加了以下功能：

1. 发布日期：于 2017 年 5 月 23 日，美国东部时间晚上 8 点（0:00 UTC）分叉 Zclassic。
2. Equihash 算法是一种对内存有要求的工作量证明机制挖矿算法。其理论依据是一个著名的计算法科学及密码学问题——广义生日悖论问题和 Wagner 算法。卢森堡大学的 Alex Biryukov 和 Dmitry Khovratovich 共同发明了 Equihash 算法。
3. 区块奖励：12.5 ZenCash.
4. 区块产生时间：2.5 分钟
5. 区块大小：2MB
6. 难度调整算法： Digishield V3，使用了下列的尾随平均难度窗口：

$$\text{下一个难度} = \text{最后一个难度} \times \sqrt{(150\ \text{秒}/\text{最后一次出块时间})}$$

7. 每个 PoW 区块奖励的划分，矿工与其他利益相关者之间交易费用：
    a) 88%给矿工
    b) 5%给一个或多个去中心化的自治组织（DAOs）
8. 总计最终币供应：2100 万。
9. 挖矿奖励每四年减半
10. 屏蔽交易会隐藏发送方、接收方和来自区块链的数额。
11. 透明交易会公开发送方、接收方和区块链上的数额。
12. Z 交易的安全消息长度为 1024 字节：
    a) 支持安全发布内容到 GNUnet 或 IPFS 路径

b) 支持用户之间的短消息

c) 支持发布到任何拥有频道功能钱包的人都可以看到的频道。

13. 安全节点执行基础架构功能：

a) 确保节点之间的所有网络通信被加密

b) 同步完整的 ZenCash 区块链为 ZenCash 钱包应用程序提供基于证书的加密连接

14. 达到要求的安全节点会得到币本位的奖励。

15. 使用商业化 CDN 进行 Z 交易的 Domain Fronting 服务。

16. 由一个或多个 DAOs 治理（详见“治理”篇）。

17. Zen DAOs 为负责系统的运行和持续改进。它们将建设和运行：

a) 有关 Zen 的信息发布（Web、维基、博客、媒体）

b) 提案制和投票制度

c) 报告和检测系统

18. 核心团队：

a) 包括 Zen 的创始人

b) 以指导执行、早期成长与发展为使命

c) 为今后的发展和维持提供关键资金

d) 在 Zen 系统和传统系统接口之间开展工作

4. 发展路线

“尝试和错误是一种自由。” ——纳西姆•尼古拉斯•塔勒（2012）

为了创造出一个能加速创新的系统，Zen 整合了多项革命性技术。我们要构建一个优秀的去中心化与持续的竞争体系，让系统可以跳出舒适地带并不断的发展。最初的蓝图涵盖了 12-18 个月的开发周期并可以自主运行。要做到这点，需要有一整套核心部件：包括安全节点网络，类似于 GNUnet 这样的分布式数据储存系统与更广泛生态系统，包括交易所、矿池和用户社区。ZenCash 需要做到完全可用并且易获取，同时对于各种利益相关者都有帮助。我们的蓝图设计侧重于将 ZenCash 作为 Zen 系列中首要产品，包括：

1. 开发改进的钱包

a) Windows：t、z 交易、消息传输、GNUnet 发布

b) Linux：t、z 交易、消息传输、GNUnet 发布

c) Mac：t、z 交易、消息传输、GNUnet 发布

d) 移动设备（安卓与 iOS）t、z 交易
e) 硬件钱包：t、z 交易、消息传输、GNUnet 发布
f) 网页钱包：t、z 交易、消息传输、GNUnet 发布

2. 使用商业化 CDN 进行 Z 交易的 Domain Fronting 服务。
3. 建立于可快速恢复的多数据中心之上的 Zen 系统服务器
4. 基础架构恢复力的测试、检查结果与改进
5. 隔离见证的实施
6. 治理研发的可交付成果，包括经过充分测试的运营体制（详见“治理”篇）：
   a) 研究报告
   b) 宪法
   c) 经过测试与实施的投票制度
   d) 第一个通过至少一个 DAO 审查的选举出的核心团队

5. 功能组件

Zen 将许多不同的要素整合在一起形成了一个整体。Zen 需要的是安全节点，而非常规节点，这样可以确保节点标准会高于基本的安全性标准，使整个系统保持分布式、快速恢复和安全。通过加强节点之间、节点与钱包之间的加密通信能力，Zen 对窃听和中间人入侵进行了防范。

Zen 同时也解决了其他加密货币的元数据缺点。例如，由于比特币交易的参与者是在一种有潜在危险的方式下通信并传输比特币，因此他们有存在被其他交易相关者识别出来的风险。因此，

- ZenCash - 将在屏蔽交易中纳入安全消息机制，用户可以确认交易、发送、验证收据。这些功能要素将体现在下列系统中：
- ZenChat - 一种新型的安全通信网络，能够通过区块链来进行一对多通信，并永久储存消息
- ZenPub - 使用 GNUnet 或 IPFS 的匿名文档发布平台
- ZenHide - 通过 Domain Fronting 技术突破加密电子商务的封锁

5.1 T 交易

T 交易是传统的由钱包里的私钥控制的区块链交易记录。这来源于比特币，并能够与交易所、钱包和其他比特币衍生的生态系统应用程序快速兼容。

5.2 Z 交易

Z 交易的概念来自于 Zcash 和 Zclassic，是会被发送到受保护地址（z 地址）的一种交易。z 地址里的余额属于隐私。当发送到一个或多个 z 地址时，该余额将保持非公开状态，但接收端的任何常规地址（t 地址）会公开此次交易的令牌并显示区块链上接收到的数值。无论该币是从一个还是两个 z 地址发出的，这些发送方的 z 地址在被公开时仍会是保密状态。Zcash 协议里详细描述了该过程：

> Zcash 里的交易分两种：常规的和受保护的。通过 t 地址转账基本上与比特币具有相同的隐私级别。z 地址通过票面（note）传输，该票面包含了金额和支付钥匙。支付钥匙是接收地址的一部分，接收地址便是这些票面被发送的目的地。与比特币一样，这和私钥相关联；私钥可用于花费被发送到地址的票面。在 Zcash 里，这被称作花费私钥（spending key）。
>
> 每个票面都对应了一个被加密的票面签章（note commitment）和一个注销符（nullifier）（在记号、记号承诺和无效符之间是 1:1:1 的关系）。计算这个注销符需要相对应的花费私钥。若连花费私钥都没有，则无法将票面签章与相之对应的注销符联系起来。一个未被使用的有效票面被定义为：在一个给定的区块链快照上，一个已公开的票面签章但与之对应的注销符尚未被广播。
>
> 和比特币协议运作得一样，每一笔交易包括了透明的输入、输出和脚本，和一个由零或多个 JoinSplit 描述组成的序列。每一笔交易描述了一次 JointSplit 传输：接收一个透明值和至多两个记号，并产生一个透明值和至多两个输出记号。输入票面对应的注销符被公布的同时（防止该票面被重复使用），输出票面的票面签章也会公布（以供以后使用）。每个 JoinSplit 描述还包括经过计算的 zk-SNARK 证明，该证明几乎可以完全保证以下内容：
>
> - 输入金额和输出金额相等（单独针对每次的 JointSplit 传输）
> - 每个交易输入的注销符都有与之对应的公开的票面签章
> - 发送方知道输入票面的花费私钥。
> - 注销符和票面签章都计算无误
> - 为了防止不持有私钥的一方修改交易，输入票面的花费私钥通过加密的方式和整个交易的签名联系在了一起。
> - 每个输出票面的注销符都不能作用在其他票面签章上

在 zk-SNARK 之外，能够确保了输入票面的注销符还尚未被公开（即它们还未被花费）。

一个支付地址包括两个钥匙：一个对应票面被发送到的地址的支付钥匙，和一个于“key-private”非对称加密体制的传输钥匙。“Key-private”的意思是，除了私钥持有者之外，密文不会向其他人公开其加密的钥匙的信息，（此处，又称之“视钥（viewing key）”）。这项功能的用途是：将区块链上被加密的票面发送给目标接受者，目标接受者可以使用“视钥”来扫描该这个票面并进行解密。

Zcash 的隐私属性的关键在于：当一个票面被花费后，花费者可以证明该票面对应的票面签章已经公开但无法被别人知道是哪个票面被公开了。这样就可以做到一个已经被花费的票面无法再与创造它的那次交易关联上。从对手的角度来看，若要追溯一次交易里的某个票面，则需要追溯包括以前使用过的所有票面集合，而这是对手方无法控制或知情的。这一点和下面的观点相形成了对比：一些私密支付系统（例如 CoinJoin、CryptoNote）的做法是要建立在有限数量的交易上，这样做会减少的可追溯性票面集合。

注销符是对“双花”的关键：每个记号只对应一个有效的注销符，因此若同一票面被使用两次，它的注销符也会被公布两次，因此第二次交易就会被拒绝。

5.3 ZenChat

ZenCash 的 Z 交易能够支持发送加密的文本消息并被记录在区块链上。这些消息的长度有 1024 个字符长度的限制，文本消息增强了用户进行安全商务的能力。用户可以选择 Zen 而不是隐私保护效果一般的其他通讯渠道来进行有关商务的讨论。在涉及小数额 Z 交易的受保护转帐的前后，用户可以使用 ZenChat 消息来和对方交流。这些消息可以直接从一个 Z 地址发到另一个 Z 地址或者一个频道。用户可以订阅一个 z 地址，这个 z 地址是通过频道名字的生成的散列，然后可以收到任何人发布到该频道的任何内容。

例如，频道#ZenCash_announcements 的散列值会是 zXXXXXXXXXXXX，所有用户都可以向该频道发送一个匿名的消息。每个消息的发送都会花费一定量的 ZenCash（因为它是包含在 Z 交易里的），这样会减少公共频道上的无用消息。官方公告将由私钥签署并且只在被认为是有效的情况下才会显示。另外，可以通过创建一个复杂的频道名字，然后用只有目标接受者持有的钥匙对消息内容加密，这样私密的群消息就能通过 Z 交易被发布出来。ZenChat 消息将使用诸如 Perfect Forward Secrecy（PFS）的 AES-256 等算法进行加密，以符合当前安全通信的加密标准。

5.4 ZenPub

在 Z 地址的文本字段中发布一个符合 IPFS 或 GNUnet 标准的地址就能够完成向 IPFs 或者 GNUnet 发布文件。目前首选的文档发布系统是 GNUnet，因为它提供了匿名发布所需的基础架构，并维护了一个文档的活动数据库。ZenPub 同样可扩展到 IPFS 或任何未来可能出现的分布式归档系统。通过结合匿名消息功能和匿名文档发布功能，ZenPub 实现了真正的匿名发布，这样消息可以快速地分发给感兴趣的读者。

5.5 ZenHide

在一些反对加密商务的国家，监管机构有可能会屏蔽像比特币甚至 Zcash 这样的传统加密货币。Zen 使用域名前置（Domain Fronting) 技术来确保在不利的网络环境下完成交易，以下是域名前置的有关于抗通信屏蔽的部分摘要：

> 通过掩盖一次通信的连接端点，“域名前置”被描述为一种多功能的规避审查技术。域名前置位于应用层面，使用 HTTPS 协议，假装与被允许的主机通信，实则与被禁止的主机通信。关键思路是在不同的通信层使用不同的域名。有一个域名会显示在 HTTPS 请求的“外部”——DNS 查询和 TLS（SNL）拓展，还有一个域名显示在“内部”——HTTP 主机头，后者在 HTTPS 加密下对检查器不可见。
>
> 审查者无法识别一次通信的域名是否被前置，只能在允许规避传输和完全屏蔽所有域名中选择，后者将导致巨大的附带损失。
>
> 域名前置易于安装和使用，不需要网络中介的特殊合作。我们已经知晓一些难以屏蔽的网页服务，譬如内容分发网络，它支持域名前置连接，利于规避审查。

在 Zen 推出时，域名前置的具体实施借助了商业内容分发网络（CCDN）。在我们整体架构最初设计已经考虑了灵活性，因此随着技术发展，该系统还有很多可能的拓展方向。

5.6 Zen 安全节点

安全节点是区块链里的关键角色，它维护了区块链的运作、接受来自钱包的交易、确认矿工挖矿算法的有效性、扮演了加密货币的去中心化的计算和通信系统的角色。在 Zen 里面，所有进出安全节点的信息都由使用 TLS 1.3 的有效证书加密，接着又由 Perfect Forward Secrecy（PFS）保护。安全节点的存在的一部分意义是可以使基于 ZenCash 的应用得到如下提升：

- 拓展 PRC 以使 AES 加密数据驻留在私有交易中。

- 拓展 PRC 以使公钥之间有 PFS 信号交换。

符合所有要求的安全节点会以排队方式按预设好比例从挖矿收益中获得奖励。安全节点需要随时听候于#secure nodes 频道。安全节点支付系统的运行细节是可审计且透明的，对安全节点的最大化可用性和最小化故障率提供了明确的标准。

1. 安全节点基本的基础架构功能：
   (a) 确保节点间所有的网络通信都被加密
   (b) 维护完整的 Zen 区块数据
   (c) 为 ZenCash 钱包应用提供基于证书的加密连接
2. 符合以下要求的安全节点会得到基于可用率计算的报酬——3.5%的区块奖励：
   (a) 在达到基础架构配置要求的系统上运行节点软件。
      - 建议大于 4GB 的内存

   (b) 维护完整的 ZenCash 区块链运行
   (c) 向 ZenCash 节点软件提供有效的 SSL 证书以使其和其他节点、钱包交流
   (d) 需要至少保存 42 个 ZenCash 在一个 t 地址中，作为押金
   (e)大约每十分钟对 SecureNodeHQ 发布在 SecureNode 频道里的挑战测试消息待命（在 z 交易消息字段中）。
   (f) 对挑战消息做出回应并带上自我身份验证信息
   (g) 挑战测试回应由两方面组成：
      i. 向 SecureNodeHQ 发送一个包含公共 t 地址和并在消息字段里附上 GNUnet 文件位置的私有消息。
      ii. 向 GNUnet 发布一个由私有 t 地址签署的文件：
         A. 也会用作奖励支付的 Zen 的公共 t 地址
         B. SSL 证书和 IP 地址
         C. 区块链的区块头
         D. 能提供服务器唯一识别性的其他信息

   (h) 每个 Zen 安全节点都必须是 GNUnet 系统上的一个端点，以匿名形式发布挑战测试回应并且支持接受来自该其他端点的匿名消息发布。
   (i)未来可能会出现其他潜在要求，以使 ZenCash 系统通过安全节点达成一致和获取计算能力。

3. Zen 安全节点支付系统（Z-SNPS）：

(a) Z-SNPS 由一个 Zen DAO 运营

(b) Z-SNPS 追踪来自每个安全节点的挑战测试回应

(c) 安全节点会被通过 t 地址追踪并发布

(d) 挖矿的块收益将向 ZC-SNPS 系统支付 3.5%的报酬，该系统将根据安全节点在一段时间段内的可用率将 ZenCash 定期分发到安全节点。

因为 Zen 的分布式计算网络是基于有报酬的安全节点的形式存在，因此这些节点可能需要根据社区共识的演变为网络提供其他计算服务。

5.7 Zen 标准节点

ZenCash 应用可以在任何 linux 服务器、Mac 或 PC 上使用。客户机同时扮演着节点和钱包的角色。虽然它没有像 Zen 安全节点一样的完全加密功能，但所有节点都有助于系统功能有效运行，并且保持遭受攻击后的恢复力。

5.8 ZenCash 钱包软件

ZenCash 软件可以用作钱包操作。命令行钱包是基本形式，同时基于桌面的操作系统上已经存在图形用户界面（GUI）的版本。手机、网页、Rasberry Pi 和其他硬件钱包会优先开发，以增强用体验和 ZenCash 代币的安全性。通过钱包的配置文件，可于任何工作中的 ZenCash 节点来进行通信，也可以将钱包设置为仅连接到安全节点，以保持高标准的信息安全。

5.9 应用

Zen 是我们认为的优秀的去中心化开源项目，所以我们希望该应用的开发能够由多方完成，一起对生态系统做出贡献。许多贡献很可能会以自愿的开源方式做出，但是我们期望一个强大的商业社区也能在围绕平台成长。此外，核心团队已经有一个正在进行中的完整的应用开发计划。这个计划包括但不仅限于：

- 节点应用
- Equihash 开源矿池
- 治理应用
- 监控报告系统
- 各类钱包
- 安全节点监控系统
- 安全节点支付系统

6.治理

“思想从而降生：以实例展示一条更好的道路远比使用暴力要好的多。 “—— 乔• 夸克，海洋家园研究所

Zen 是一个去中心化的治理模型，其中包含了多方利益相关者的授权许可，和在逐渐演化发展中更好地适应我们社区的灵活性。一般来说，我们所理解的治理就是我们无法根据事先预测得出最好的办法，只能通过脑中的想法去推动项目的施行，从而使其满足社区所需。我们相信治理既是服务也是目的，旨在为直接利益相关者、更大范围的社会甚至世界提供更有效的价值。

“任何一个只追求利益而忽视服务的行业都应该被淘汰。”（夸克，2017）治理就是一个很好的例子。我们拒绝强制性的集中并主张自愿原则，这与当今世界上的主要想法与项目是一致的。我们相信每个人都享有自由，而不是只有少数有权之人才能享有。

我们的治理模型核心在于权力的去中心化从而使内容与创造性达到最大化。现行的实践方案必须认识到：大量的资源与精力投入应产生协同作用，从而进行平衡以避免完全的去中心化；优化重点应处在时变状态，并由自愿的参与和退出来决定。

重要的是，我们正在运行一款系统。在这个系统中，相互竞争的 DAOs 可以分享资源，甚至可以归化一些低效过时的版本。因此，我们不应该只有一个在不同环境、时间、功能、文化下一成不变的通用型版本的结构，而应该有许多可供选择的结构。它们具有流动性和灵活性，适用于特定的情况，能随着工作和环境的变化而变。这种系统的巨大发展使其可以匹敌具有竞争力的反馈信息。

在治理方面，我们追求的状态是平衡去中心化，提高实施效率，分散权力，扩大相关利益者的授权，实现灵活的变革。实现这一初级状态需要至少 12-18 个月的研究与开发，并在博弈论、政治科学、以及经济研究上作出努力。其中，在经济研究方面采用理想的投票机制与从大量的测试网络实践中得出的反馈信息相结合的方式进行研究。此项目将是我们投入资金后产出的第一个成果，其中包括了全面的研究报告与融入 Zen 网的操作码。在为期六个月的治理运行中，我们希望可以通过全面公开的选拔选出第一批操作领导团队。

6.1 理想的去中心化

“一个叫做加密无政府主义的幽灵正萦绕在现实世界中。”——《加密无政府主义者宣言》

我们认为，通过去中心化的方式，每个人都享有平等的参与机会。这样也可以最大化分散决策权力，使得系统产生抵抗捕捉信息的行为。从理论上讲，最大化去中心化指每个个体对决策具有平等权力。但在实践中，将大量的资源信息放入同一个系统中是很难施行的。对于特定的利益相关者而言，即便是在纯粹的环境下实施去中心化，合作资源与效率的个人决定池仍存在不平等的比率。

我们无法阻止自然力，也不能认为这些自然力是有害的。我们能做的是设计一个自愿参与的系统，使得建立在资源配置上的决定权力与典型的利益相关者相平衡，之后在信用机制中的得出反馈。其次，我们明白具有灵活性的结构比万能不变的结构更重要。尤其是我们正在不断扩展范围，这也证明了预测未来是不太可能的。对于去中心化组织来说，施行效率也是一个很大的问题。纯粹的分散可能会导致决策瘫痪，选民态度冷漠，极高的群体幻想。这就是为什么我们一开始在决策上避免纯粹的民主，我们选择研究竞争性模型，并在不同压力情况下对它们进行测试。我们对 DAOs 所设置的自由开放的环境，旨在鼓励高绩效功能领域的专家和小组可以在其专业领域发挥领导力，使我们的系统可以提高转化资源到高价值产品，提高服务的效率来不断满足用户的需求。

6.2 检验与平衡

人类的发展历史教会我们最重要的一课是要明白权力应最大化去中心化，权力集群应提供一种检验与平衡间的均势状态。平衡应适应于任一权力集群中的无抑制性增长，这样整个系统会更易于捕获。为了在初期就避免这种情况，Zen 推出了一支“核心团队”来控制 3.5%的块奖励资金，最初的 DAO 包括了控制着 5%的资源的行业领导者。除此之外，我们的目标状态是在 12-18 月的研究与开发和测试阶段中包括多个利益相关方投票的混合状态。以至于有代表性的社区可以保留权力来影响决策和资源分配。最终，我们治理结构的各个方面都会受到竞争性反馈和变化的约束。我们正在采取一种渐进的方法，即从一个伴随社区发展的简单模型入手。

7.DAO: 基础架构，方案与投票

Zen 系统将至少有一个由挖矿收益中按固定比例资助的 DAO，这个 DAO 由一个投票系统所管理，所有利益相关者都可以参与投票。该管理制度有助于减少在项目的更改、改进和集成的实施上产生的争议，以降低由分歧导致分叉的几率。我们会执行在过硬的研发和测试中所学到的更全面的治理计划，该计划的目标是在治理上要开放全面竞争，以至于每个人都能参与。这就意味着我们将看到大量相互竞争，为解决不同问题，由不同工作团队组成的 DAOs 出现。每一个

DAO 都会有自己的结构，流程和目标，以确保它们各自的属性通过竞争而发展，那些一开始就伴随着错误的组织决策便不会永久存在。

我们的 DAOs 将负责构建，维护，改进和保持基础架构，以保证系统得以运行。它还会负责运行 Zen 软件应用程序的更改，并且具有足够的灵活性来支持其他社区的重要事项，例如社区外延服务，营销，培训等。

随着 Zen 系统的普及，用户、矿工、安全节点操作员和生态系统合作伙伴也需要扩大规模。DAO 这样的结构可以将资金分配到各个项目和建议，来支持其发展。
我们鼓励社区以不同的方式对 Zen 做出贡献。DAOs 负责管理协调社区所作出的各项贡献，并提供资金来支付在此过程中社区可能产生的开销。这样做的目的之一是补偿社区成员在支持和帮助系统的运作中所产生的成本。

在启动之时，Zen 将配有一个由通晓多个相关行业知识人员的 DAO。当管理计划准备实施时，这个 DAO 团队同样会和任何想要建立起自己的组织的团队一起竞争，最终决定会由整个社区做出。

7.1 由 DAO 所运行的 Zen 基础架构

DAO 系统将维护应用服务器和服务，包括：

- 安全节点验证服务器
- 论坛服务器
- Slack
- 网站
- 博客
- 提议系统
- 投票系统
- 代码管理仓库

DAOs 将提供以下支持：

- 帮助人们使用 ZenCash 或其他系统功能
- 帮助安全节点操作员
- 排查节点奖励问题
- 排查投票系统问题
- 提供升级支持

- 提供快速和最终问题的仲裁

在成功投票和否决期满后，DAO 将 ZenCash 分配给提案所有者。

最初会有 3-5 个 DAO 的负责人，但这没有限制。负责人也可以匿名，但不做硬性规定。实际上，公开身份可以将曾经的专业成就和品格优点自然地带到 Zen 系统中，这是一个好事。争议是一定会出现的，因此我们需要制定解决机制来有效并公正地做出裁决。在治理研发项目（Governance R&D ）中将会探讨建立司法和陪审制度的可能性。

7.2 建议提交与投票

每个 DAO 都有自己的结构，流程和优先事项，除此之外，它们有一个共性，也就是会有一个自由、开放的系统，该系统是为工作、评估及奖励机制而设立的。我们没有明确理由为什么会有这个系统，因为就该有。这是一个面向全人类的开放社区，这里不应该设立准入门槛。我们为初始的 DAO 提出的建议以下：

1. 每两个月投票一次。投票前两周为提按提交截止日期。投票日期：1 月 31 日，3 月 31 日，5 月 31 日，7 月 31 日，9 月 31 日，11 月 31 日
2. 投票后公开提交的建议。
3. 否决——核心团队可以在投票后 7 天内以全票行使团队否决权（不建议做此决定）。
4. 为提议提供的资金按照投票当日以 ZenCash 的当地货币汇率为准（防止出现像 DASH 那样因为价格快速上涨而导致项目遭到拒绝）。
5. 投票使用代币。投票前 1 个月会分发 1440 个代币。
6. 大多数提案超过 720 代币持有者投赞成票即通过。
7. 某些提案需要绝对多数投票（大于 1080 票）才能通过。

7.3 投票过程

代币分配计划——在投票期间，总共有 1440 张代币：

1. 360 个代币供出售——允许用户和 ZenCash 持有人购买。.
   (a) 1-30 个代币：售价 1 ZenCash
   (b) 31-60 个代币：售价 2 ZenCash
   (c) 61-90 个代币：售价 3 ZenCash
   (d) 以此类推，最高售价 12 ZenCash
2. 240 个代币——分配给 ZenCash 项目开发者
   - 为提交代码（commit）、贡献代码（pull request）或其他合理的贡献措施给予奖励。

- 目的是提高软件和系统开发人员相关权益。.

3. 60 个代币——上市 zencash 的交易所
   (a) 交易额前十名者每人获得 10 个代币
4. 60 个代币——挖矿池所有者
   (a) 每 480 个块中奖励一个代币给找到块的矿池
5. 360 个代币——安全节点
   (a) 每 40 块奖励一个代币，直至 360 个分发完。
6. 120 个代币——平分给 DAO 执行官
7. 240 个代币——平分给核心团队

8. Zen 核心团队：基础和领导

核心团队最初由该项目的三位早期创始人 Joshua Yabut，Rob Viglione 和 Rolf Versluis 组成。每位创始人都是其各自专业领域的领导者并拥有过硬的经历和专业的加密货币知识。

Joshua 是一位经验丰富的红队成员和前航天工业应用开发人员。他热衷于开发抗审查网络和喜欢重新定义现状。他拥有攻击安全认证专家（OSCE）认证，德保罗大学 IT 项目管理硕士学位，并拥有在开发管理和协作网络方面具有丰富的知识。Joshua 有广泛的加密货币开发经验，曾带领 Zclassic 的核心团队开发了 z-nomp 矿池协议，支持 ZCash 开发社区，始终如一得提供优质软件。

Rob 是一位前物理学家，雇佣兵数学家和在卫星雷达，太空运载火箭和作战支援情报方面有经验的军官。在加密货币领域作出的贡献包括：Zclassic 核心团队的一员，支持 Bitshares 项目，负责 BlockPay 的美国项目＆加拿大大使计划，担任 Bitgate 的顾问工作。他目前是金融 @UofSC 研究的博士候选人，在该教育机构教授“比特币和区块链在金融领域的应用”。Rob 拥有一个金融与营销的工商管理硕士和 PMP 认证。他是一个热情的自由主义者,主张和平，自由和尊重个人生活

Rolf 是 IT 行业的经验丰富的企业家，在佐治亚州 Alpharetta 拥有一个中等规模的比特币和 Zclassic（ZenCash）挖矿业务。有在思科系统，半导体行业以及在美国海军陆战部队的核训练官员的经验，Rolf 给 ZenCash 组织带来了领导力，管理和操作技术方面的专业知识。

为了完成早期的路线图，包括快速部署系统并最终形成一个可全面运作的网络，Zen 建立了一个具有决策权的核心团队实体和独立预算系统，我们最终的目的是通过研发向更广泛的治理结构过渡。我们的目标是在完成初步路线图并按照治理计划通过选举成为一个 DAO。 到那时，我们将在届时的 DAO 中开展办公业务，或考虑启动我们自己的 DAO 系统参与到整个竞争系统中。

9. Zen 社区：强大与活力

Zen 与 Zclassic 项目共同演进，我们的共同社区约有 1000 个论坛成员、开发商、矿工、交易员、长期投资者、合作伙伴组织、交易所、博客使用者等。作为一个全面开放和包容的项目，Zen 收到了来自全世界的贡献和支持，这种即时性和意志包容性也是我们所定义的系统特点之一。我们的社区不仅有积极友好的互动关系，还有自发的支持和参与，以避免或解决不同的问题。

9.1 公开源代码中的伦理道德

公开源代码会逐步形成一套伦理问题,然而创始人希望社区保持以 Zen 原则为中心，正因如此才有 Zen 这个名字。我们希望这个正在开发的系统可以用于和平协作，允许创新和最大限度包容的系统。我们希望这个产物将对社会有益，我们个人拒绝与任何有意图伤害他人的人进行合作，不论是人身攻击还是欺诈行为。

9.2 Zen 支持服务

Zen 支持服务是指 Zen 开发人员和其他 IT 专业人士，他们致力于推动技术并向用户提供基本帮助。该网络将由 DAO 资助，使 Zen 的技术以直观得，好用得参与到生态系统中。其次，Zen 支持服务还将包括来自不同行业的使者，导师组成的贡献者网络，以对 Zen 贡献者进行支持。这些可以在随后的 Zen 社区部分中查看更多内容。Zen 支持服务组织结构的设计旨在促进包容，协作和集体援助，以此使得 Zen 使者，Zen 企业家或任何 Zen 社区的代表成为赖以合作的贡献者。

9.3 Zen 外展服务

我们的规划图包括前所未有的外展服务计划，这将加强我们与各界人士的接触。简而言之，Zen 没有一个单一的“目标市场”，当我们的技术实际应用案例和我们的技术变得多样广泛时，我们该怎么做呢？我们不打算以核心团队成员的个人想法给 Zen 的使用划定界限，因此我们将启动一个项目，旨在最大限度地与 Zen 产生接触，并让社区成员在 Zen 发展进化时适应我们的任务和举措。最初的 DAO 正在保留资源为实验计划提供资金，并奖励那些积极在社区中做出贡献的成员。其中一些提议的方案想法将会在下文阐述。

再次声明，Zen 具有包容性和不可知性，我们的全球影响力将反映出这些核心价值观。我们的组成中将有各种利益集团，包括企业家，积极分子，开发商，大学，公司和不知情但充满好奇的个人，他们在加密货币的世界里留下了积极的活动记录。

通过我们的 **Zen 大使项目（Zen Ambassador Program）**，有经验的用户，思想领袖和热情的社区成员将被授予代表 Zen 的机会，向世界各地原本无法获取资源，资本，技术的人们表达我们的愿景，希望他们能够主动加入社区。该项目的领导者可以起到许多作用：为 Zen 创业公司提供建议，指导 Zen 章程，在新闻界代表 Zen。

通过参加我们的 **Zen 青年项目（Zen Youth Program），**全球青年可以获得集中编码和商业发展的教育培训，也会获得参与 Zen 集体接触的宝贵机会。这个项目将是多方面的，其中包括在 Zen 平台上的由 DAO 赞助的创业比赛，或者乐透式分配奖金资源以支付 Zen 青年的教育费用。这些优秀的年轻人也将被动员起来招募他们的同龄人参与社区活动。

管理 DAO 资助项目的企业家将会成为 **Zen 认证企业家（Zen Verified Entrepreneurs），**并获得相关的创业加速器的特权，有机会接触到例如成功的商业导师、营销和用户获取渠道，接触到参与开源项目的开发人员、获得直接与投资者和风险投资公司接触的渠道，以及接触到到旨在协同解决问题和促进创新的活动，合作伙伴关系和研讨会。

个体贡献者将有机会获得即插即用的内容以适应当前不断扩张的草根运动，以 **Zen** 社团（**Zen Chapters**）的形式在全世界范围内改变他们对 Zen 技术、伦理道德、治理以及开发项目的看法。Zen 社团是本地化与可定制的，其重点取决于地区和社区需求。Zen 将提供一个基础的物质资源在线平台，其范围包括：

- 市场营销与教育板块，其详细介绍了 Zen 的起源、具体特点、差异和目标。
- 为希望创建 Zen 赞助的促销或教育活动的团队提供会议和比赛的模板和想法。
- 基于 Zen 原则下的模块、讨论、在线研讨会以及可供社团加入的相关课程：编码、企业家精神、去中心化的伦理学，区块链的基础等等。
- 提供业务计划数据库，法律文件，收入模式，用户获取策略等，以供社团进一步开展业务发展计划或努力改善社区。
- 通过 Zen 渠道获得 Zen 贡献者和开发者的支持，建议，指导和帮助。

例如，在菲律宾大约只有 30%的人可以获得金融服务，在那里的 Zen 社团可以实际参与到满足菲律宾人特殊需求和国家文化与基础设施规范的国际共同开发的 FinTech 项目中去。实际上，

这个可伸缩的活动会很大程度地减少一些摩擦，这些摩擦在历史上阻碍了社区自主地发展其小规模经济，也阻碍了其竞争力的增强。

在 21 世纪，虚拟互动和沟通的发展是非常有价值的。这也将成为一个核心渠道，可以连接相隔数千公里间的人们，使他们共同促进 Zen 的创新与发展。话虽如此，在 Zen 的我们也意识到面对面互动仍是极好的，因为我们致力于共同的一系列原则和共同愿景。我们将在每年开始一期 Zen 大学，以奖励和吸引 Zen 最积极和最有价值的贡献者，有上进心的青年和杰出的企业家。我们还将以随机分发门票给一些高质量的 Zen 安全节点。其主题，内容和目的将根据 Zen 社区的喜好而有所不同。

我们的资源被用于我们的 Zen 社区，其中包括许多其他的参与者和活动，这将会比传统加密项目下的股东所能提供的价值更高。我们希望这个技术项目能成为一个社会运动，最终目标是帮助人们最大化地自由生活，获得更多满足。

10.竞争性展望

“我们一直认为，随着时间的推移，许多公司习惯了只慢慢地做微小进步，多数时只是反复做同样的事情。但在技术行业，你们需要变革性的点子来推动下一次大的进步，要与时俱进就不能只做习惯了的事。” ——拉里•佩奇, Alphabet

竞争是 Zen 的核心。基于其本质而言，竞争是最理想的去中心化的必要条件，我们认为竞争也可以促进 Zen 的发展。这个过程还包括使 ZenCash 这个加密货币在更大的范围内竞争，和 Zen 在区块链生态系统中的竞争。ZenCash 与 ZCash,Zclassic,Dash,Monero,ZCoin,比特币,ShadowCash,Boolberry, 和一些其他匿名增强型加密货币直接竞争。尽管竞争面十分广，但从技术的角度来看，我们直接与基于 zk-SNARKs 的零知识货币进行竞争。Zcash 是这一领域的先驱者，我们的技术直接受益于其突破性的贡献。Zen 在隐私功能方面存在许多竞争对手，如 Zerocoin 协议, CryptoNote, RingCT 和一些更简单的混合体。事实上，所有这些虚拟货币都在加密货币的需求曲线上满足着特定私人用户群体。

我们的价值主张是主动吸收我们所认为的最佳元素，从起初继承于零知识 Zcash 的实行，并通过 zk-SNARKs 进行保护，然后我们迈出了关键的一步，通过端到端加密混淆整个网络，使消息可以以目前最安全的基础设施中传递。重要的是，我们计划与时俱进，因为我们已在结构上做好了准备。不仅仅是跟随最新技术升级和更新我们的系统，更是为了成为行业中的创新者。

Zen 正在建立一个以 ZenCash 作为代币或燃料的体系结构。就这点而言，我们还将与广泛的平台式项目进行竞争，如 Ethereum，Ethereum Classic，NEM，Lisk 和 Synereo 等一类建立在去中心化应用之上的项目（dApps）。在这方面，从比特币和 ZCash 继承的简单脚本语言使 Zen 获得了可抵御一系列向量攻击的安全性和快速恢复能力，但同时这也限制了更复杂指令执行的自由度和执行增强的图灵完备的脚本的能力，就像 Ethereum 和 Ethereum Classic。我们在这个竞争领域的优势在于，dApps 可以建立在世界上最安全的加密网络之上，而且我们具有足够的灵活性，能够通过战略合作来达到可跨链运行。

我们竞争力强劲和变革性的治理模式是我们对加密货币体系的独特创新，以在去中心化的环境中广泛授权利益相关方。比特币在分布式一致性上实现了原有的突破，但其他加密货币项目已经进一步融入了各种投票机制。这些项目的投票机制包括，Dash 的简单提案和社区投票模式，甚至 Decred 的嵌入式社区治理；各方都对去中心化一致性作出了积极的贡献。但是 Zen 又做了进一步发展，它放宽了额外的制约因素，在生态系统内的治理服务提供商长期互相竞争下，我们的系统也可以随着时间的推移继续发展。我们正在实施一个自主的系统，它可以在去中心化系统如何组织起来解决具体的问题下，随着不断地反馈、试错的创新而变。在这个层面上，我们相信 Zen 在社会技术上实现了突破，开创了一个从未大规模尝试过的系统。

从更广泛的角度来看，Zen 正在与现有货币和银行体系以及新兴的 FinTech 创业公司竞争，新兴的 FinTech 创业公司旨在为被权利降级的人提供服务。我们将通过不断加强的隐私性和安全性，为这个创新的、以社会福利为导向的领域做出贡献。作为安全的信息和分布式数据存档系统，我们与其他服务商也在竞争，例如 Signal，Telegram 和 Tor Project。还有很多有潜力的项目可以建立在 Zen 平台上，以提高我们的竞争力。

我们认为竞争可以推进一个进程的健康成长，因此我们以积极的态度迎接最大化的竞争。我们宁愿生活在一个有竞争对手的世界而不是一个没有进步的静态世界，这样我们就可以迫使我们自己加速创新。我们希望 Zen 可以融合技术和社区，将治理变为有竞争力的服务，使世界上任何人都能够参与我们的授权，合作与分散的创新体系中，为人类福祉做出积极的贡献。我们将把这个领域的老牌企业和未来的创业公司视为潜在的合作伙伴和盟友，而不是“赢者通吃”的竞争对手。

11.Zen 的发展前景

虽然预测未来是一项具有挑战性的工作，但我们看到了 Zen 以及我们正在建设的生态系统的光明发展前景。我们相信，在未来，我们所创造的去中心的、完全包容性、自发性的、灵活的

组织将比 20 世纪所流行的静止的、中心化的、通用型的组织更具有明显的优势。同时，随着密码学、自愿主义哲学和区块链技术的出现，这样的事情成为可能，我们相信很多人已经在努力着并有着创造更美好世界的愿景。尤其是当他们看到我们如何加速创新，通过给予每个人表达自己的价值观的权利来实现人类福祉。

跟随路线图，我们将会在未来一到两年实现这一愿景。这一路上我们肯定会遇到各种挑战，但是我们坚信我们的可塑性和和谐的合作会使我们一路披荆斩棘。

我们足够幸运，生活在一个充满难以想象的先进技术和新创意的创新时代，使我们得以站在巨人的肩膀之上不断努力。以下的参考文献中列出了许多专家，但同时还有非常多的不被人所知却做了很多基础工作的人们未在这里列举。

参考文献

[1] Juan Benet. (2014) IPFS - Content Addressed,Versioned, P2P File System.

[2] Eli Ben-Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. (2014) Zerocash: Decentralized Anonymous Payments from Bitcoin.

[3] Evan Duffield, Kyle Hagan. (2014) Darkcoin: Peer-to-Peer Crypto Currency with Anonymous Blockchain Transactions and an Improved Proof-of-Work System.

[4] David Fifield, Chang Lan, Rod Hynes, Percy Wegmann, and Vern Paxson. (2015) Blocking-resistant communication through domainfronting.

[5] Daira Hopwood, Sean Bowe, Taylor Hornby, Nathan Wilcox. (2017) Zcash Protocol Specification Version 2017.0-beta-2.5.

[6] May, T. (1992). The cryptoanarchist manifesto. High Noon on the Electronic Frontier: Conceptual Issues in Cyberspace.

[7] Nakamoto S. (2008): Bitcoin: A peer-to-peer electronic cash system.

[8] Quirk, Joe, and Patri Friedman. (2017) Seasteading: How Floating Nations Will Restore the Environment, Enrich the Poor, Cure the Sick, and Liberate Humanity from Politicians. Free Press.

[9] Taleb, N. N. (2012). Antifragile: Things that gain from disorder (Vol. 3). Random House.