草案

這個翻譯是草稿版本。如果您看到錯誤，並希望貢獻，請聯繫我們的團隊更新版本！

Zen 白皮书

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。结合了革命性的技术，Zen将传统意义上独立运作的三项功能融合在一起，它们分别是：交易、通信和竞争性治理，以此加速创新化。此过程采用了全球分布的区块链技术和计算基础架构，以安全、匿名的方式进行。该系统集合了多项一流技术，在这样开放的平台上，不受权限禁锢的创新可以随着用户偏好的变化不断调适、发展。

*作者们的联系邮箱分别是： rob@zensystem.io, rolf@zensystem.io, et 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

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，围绕使能技术栈建立起集产品、服务与业务于一身的平台。正当分布式的区块链影响着最新的审查规避技术、完全加密通信和长期可行的社会、治理模式时，Zen致力于维护用户的隐私权，提供了有必要的网络基础架构，用户在无边界的生态环境里可以安全地进行合作、建立价值。我们的任务是将一套分散的，温和并具有自发性的社会结构与可获取的（post-Satoshi）最新科技结合在一起，提高所有自愿参加者的生活质量。我们坚信这样的理念正是这个时代所需要的。

从整体框架上看，Zen是一个安全的、以隐私为导向的基础架构，其创建的治理系统使参与者可以共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“点对点”或“商对商”资产置换、互助团体、“点对点”保险、人道主义援助机制的去中心化、纯粹的匿名价值代币。

由于缺乏身份识别、资金和安全渠道，以上这些功能可用于为被剥夺权力的人群服务，例如银行业务和医疗保健等重要服务。希望获得所有权并通过其私人数据获利的个人也可以利用这些功能。例如，一些创业者希望建立起针内生太阳能的竞标招标制度。这样独特的应用将是无数的，只要基于我们共同的信念：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。

历史

Zen通过吸收现有的和新的特点，建立在最佳的加密货币、网络结构、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。与我们的技术栈同样重要的是：我们是基于分享共识和竞争性治理的最新思想。本项目的部分基金来自比特币、Dash、Decred和Seasteading。

Zcash扩展了比特币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）和防交通相关分析的私有地址（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关键参数：除去了20%的创始人奖励并解决了货币供应的缓慢开始。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。一些早期的成绩包括：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，有一种创新的经济和治理模式可以更好地符合Satoshi对一个分散的全球社区的独特看法，在该模式下，Zclassic可以作为一个完全加密的网络被进一步扩展。我们认为基本上Zclassic是一个纯开源的、全自愿的加密货币项目；同时，Zen也扩展成了一个有内部资金的平台，以推动更广泛的沟通、档案共享和经济活动。

执行细则

Zen是ZenCash代币散播的首要系统，类似于以太坊的代币（ETH）。ZenCash为Zclassic的一个分叉，并将扩展以下附加功能。

1. 发布日期：作为Zclassic的分叉于2017年5月23日，美国东部时间晚上8点推出（0:00 UTC）。

2. Equihash算法是一种具有记忆性和工作量证明机制的挖矿算法。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联合发明了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：微调过的Digishield V3，使用了下列的尾随平均难度视窗：

下一个难度 ＝ 最后一个难度 × √(150秒/最后一次解决时间)

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）
   (c) 3.5%给安全节点团队
   (d) 3.5%给核心团队

8. 总计最终币供应：2100万。

9. 比特币奖励每四年递减一半

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交易的安全消息字段为1024字节：
    (a) 安全发布到GNUnet和/或IPFS位置
    (b) 用户之间的短消息
    (c) 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) 保持完整的ZenCah区块链
    (c) 为ZenCash钱包应用程序提供基于证书的加密连接

14. 符合要求的安全节点会得到coinbase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 包括Zen的创始人

(b) 任务是指导执行、早期成长与发展

(c) 基金费用对于今后的发展和维持十分重要

(d) 在Zen和传统系统的交接点进行运行

蓝图

试错是一种自由。 ——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发起了革命性技术的整合，。我们要构建最佳的
去中心化与持续的竞争体系，让系统可以跳出舒适地带、不断的发展。最初的蓝图涵盖了12-18个月的开发窗口，以期系统可以自主运行。要做到这点，关键在于一体化的实现：我们自己的安全节点网络（像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需要全面投入运营，做到易获取，并且对于各种利益相关者都有帮助。我们的蓝图反应了Zen系列里ZenCash作为首要初始产品的重点。

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：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. 具有恢复力的多数据中心配置里的Zen系统服务器

4. 基础架构恢复力的测试、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) 构造

(c) 经过测试与实施的投票制度

(d) 第一次能经起至少一个DAO审查的选举成为核心团队

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，以此确保节点保持在基本的安全性标准上，系统也保持分布式、有弹力和安全。通过加强节点之间、节点与钱包之间的加密通信，Zen对窃听和中间人入侵的可能进行了防范。

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沟通并传输比特币，因此他们被其他交易相关者识别出来的风险是存在的。因此，ZenCash将在屏蔽交易中纳入安全信息，用户可以同意交易、发送、然后验证收据。这些功能要素将体现在下列系统中：

ZenTalk - 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技术绕过加密电子商务的障碍

5.1 T交易 T交易是由钱包里的私钥控制的传统区块链记录交易。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交易是由Zcash和Zclassic得来，是会被发送到私有地址的一种交易。私

有地址里的余
额属于隐私信息。如果是一个或多个私有地址，该值将保持非公开状态，但接收端的任何透明地址将公开代币和显示区块链上接收到的值。无论该值是从一个还是两个私有地址发出的，这些输入的私有地址在被公开时仍是保密状态。Zcash协议里详细描述了该过程：

Zcash里的价值既不是透明的，也不是隐蔽的。透明值的转移基本上与比特币相同，具有相同的隐私属性。屏蔽值通过字符串传输，指示了数额和支付钥匙。支付钥匙是支付地址的一部分，支付地址便是这些字符串的目的地。与比特币一样，这和私钥相关联；私钥可用于花费发送到地址的字符串。在Zcash里，这被称作花费钥匙。

每个字符串都相关联了一个加密的字符担保和一个无效符1（因此在字符串、字符担保和无效符之间形成了1:1:1的关系）。计算这个无效符需要相关的私有支出钥匙。若连花费钥匙都没有，想要将字符担保与相对应的无效符联系起来是不可行的。在区块链的一个给定点上，一个未使用的有效字符串，在该点之前已经在区块链上公开了字符担保，但无效符还没有。

正如《比特币协议》运作的那样，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。它们每一个描述了一次JointSplit传输：接收一个透明值和至多两个输入字符串，并产生一个透明值和至多两个输出值。输入字符串的无效符会公布的同时（防止该字符串被重复使用），输出字符串的担保也会公布（以供以后使用）。每个JoinSplit描述还包括经过计算的zk-SNARK证明，证明除了可忽略的概率之外，所有以下内容都是：

输入值和输出值相等（单独针对每次的JointSplit传输）

每个代表非零值的输入字符串都有公开的担保 验证方知

道输入字符串的花费私钥。 无效符和字符担保都经过正

确计算

为了防止不持有私钥的一方修改交易，输入字符串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。

每个输出字符串的出现都建立在它的无效符和其他字符串的无效符不冲突的基础上

zk-SNARK之外，也确保了输入字符串的无效符还未被公开（即它们还未被花费）。

一个支付地址包括两个公钥：一个对应字符串发送地址的支付钥匙，和一个用于“key-private”非对称加密体制的传输钥匙。“Key-private”的意思是，密文不会向其他人公开其加密的钥匙的信息，相应的私钥持有者除外（此处，又称之“视钥”）。这项功能的用途是：将区块链上被加密的输出字符串发送给目标接受者，目标接受者可以使用“视钥”来扫描该字符串并进行解密。

Zcash的隐私属性的基点在于：当一串字符被花费后，在不公开具体是哪个字符串的同时，花费者证明了相应的担保已经公开。这说明一串已经被花费的字符就无法再与创造它的那次交易相连接。从对手的角度来看，这也意味着给定字符串被输入交易的可能性集合、该次交易里的字符串的可追溯性集合包括以前使用过的字符串，而对手无法控制或知情。这一点和下面的观点相形成了对比：一些对私人支付系统（例如Coin-Join、CryptoNote）的提议是要建立在有限数量的交易上，这样也就有了更少的字符串可追溯性集合。

无效符是对付“双花”的关键：每串字符只对应一个有效的无效符，因此若同一串字符被使用两次，它的无效符也会被公布两次，第二次交易就会被拒绝。

5.3 ZenTalk

ZenCash的Z交易能够吸收那些被加密并涵盖在区块链上的基于文本的消息。这些消息有1024个字符的限制，增强了用户进行安全商务的能力。有一些频道达不到Zen的隐私保护级别，用户可以选择不通过它们来进行有关交易的讨论。在涉及小数额Z交易的私有传输的前后，用户可以使用Zentalk消息来和其他方交流。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。用户可以通过从一个频道名字的散列生成的Z地址订阅该频道，然后可以读取任何人发布到该频道的任何东西。

例如，频道#ZenCash_announcements的散列会是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），因此减少了公共频道上的无用消息。官方公告将由私钥签署并且只在有效的情况下显示。另外，通过首创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，基本上私密的群消息就能通过Z交易被发布出来。ZenTalk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

Zen能够向IPFs或者GNUnet发布文件。这通过在Z地址的文本字段中发布IPFS或GNUnet地址来完成。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。该系统同样可扩展到IPFS或任何未来的分发归档系统。通过在创建匿名消息层的同时创建匿名发布层，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Domain Fronting技术来确保在对立的网络环境下完成交易，在Domain Fronting的摘要有关于反通信屏蔽的部分：

> 通过掩盖一次通信的连接端点，“domain fronting”被描述为一种多功能的规避审查技术。位于应用层面的domain fronting使用HTTPS，假装与被检测器允许的主机通信，实则在进入被禁止的主机操作系统。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“外面”——DNS查询和TLS（SNL）拓展，还有一个域名显示在“里面”——HTTP主机头，后者在HTTPS加密下对检查器不可见。
>
> 审查员无法识别一个域名的前方和非前方的通信，必须在允许规避传输和完全阻止域名中选择，这将导致昂贵的附带损害。
>
> Domain fronting易于安装和使用，不需要网络中介的特殊合作。我们发现了一些难以屏蔽的网页服务，例如内容传输网络：内容传输网络支持domain-fronted连接并且对于规避审查有用。

在Zen推出时，Domain Fronting的具体实施结合了商业的内容分发网络，但在我们整体架构的各个方面下，灵活性从一开始也被设计在其中，因此随着技术发展，该系统可以朝着多方向拓展。

5.6 Zen安全节点

节点是区块链里的关键系统，它维持了区块链的运作、接受来自钱包的交易、确认矿工解题的有效性、扮演加密货币的去中心化的计算和通信系统。在Zen里面，所以传输来自和传输去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。作为安全节点功能的一部分，ZenCash应用通过以下途径进行改进：

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获得挖矿的安全节点部分。安全节点需要监视#安全节点频道。安全节点支付系统旨在以可审计的方式运行，对最大化可操作性和最小化问题有明确的标准。

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) 维持完整的Zen区块链
   (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受到对于全功能运行时间的奖励——区块币奖励的3.5%：
   (a) 在基础架构要求指定的有能力的系统上操作节点软件。

   建议大于4GB的内存

   (b) 维持系统里完整的ZenCash区块链
   (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) 一个t地址至少保存42个ZenCash在服务器上作为押金
   (e) 大约每十分钟对SecureNode频道里的来自SecureNodeHQ的challenge消息

监控一次（在z交易消息字段中）。

(f) 通过鉴定安全节点的信息对challenge消息做出回应

(g) Challenge response由两方面组成：

i. 向SecureNodeHQ发送一个包含公共t地址和消息字段里GNUnet文件定位的私有消息。

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. 能证明服务器独特性的其他信息

(h) 每个Zen安全节点都必须是GNUnet系统上的对等体，以匿名形式发布challenge-response并且支持来自该系统其他组件的匿名发布。

(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challenge-response

(c) 安全节点会被它们的t地址追踪并发布

(d) 矿区将向ZC-SNPS系统支付3.5%的报酬，该系统将根据其在规定时间段内的正常运行时间将ZenCash定期分发到安全节点。

因为Zen的分布式计算网络是以被酬报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或者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，但是桌

面上已经存在基于图形
用户界面（GUI）的版本。手机、网页、Rasberry　Pi和其他硬件钱包高度优先于立即开发，以增强用户体验和ZenCash代币的安全性。钱包的配置可用于通过任一可获得的Zen-Cash节点来进行通信，或者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是我们认为的最优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。许多这些贡献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

管理

“因此才会出现这样的思维方式，即举出实例的说服远比使用暴力要好的多。 ——乔•夸克，海洋家园研究所

Zen是一个去中心化的管理模型，其中包含了多方利益相关者的授权许可，其灵活性在逐渐发展中更好地适应我们的社区。一般来说，我们所理解的管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。我们相信管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）管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。

我们的管理模型核心在于权力去中心化从而使内容与创造性最大化。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抗争具有竞争力的反馈信息。

在管理方面，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。在为期六个月的管理运行中，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 最理想分散化 “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，这样整个系统会服从于采集之下。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制约。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。

DAO：基础架构，方案与投票

Zen系统将至少有一个由部分挖掘奖励资助的DAO，并由一个可以聚集所有利益相关者的投票系统所管理。该管理制度有助于确保更改、改进和集成的实施，从而实现最小化争议并减少在一个项目中由分歧导致分叉的几率。当我们展开从严格的研发和测试中所得的更全面的治理计划时，我们的目标是面向全面竞争，开放治理环境。这就意味着我们将看到大量相互竞争的DAOs伴随着不同工作团队面临的不同困难而生。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，那些伊始的、错误的、有组织的决策便不会永久存在。

我们的DAOs将负责构建，维护，改进和保持系统运行的基础架构。它还负责运行Zen软件应用程序的更改，并且具有足够的灵活性去适应其他社区的优先事项，例如社区延伸服务，营销，培训等。

随着Zen系统的普及，用户、管理者、安全的支持节点操作者和生态系统合作伙伴也需要扩大规模。DAO结构将运用资金，通过项目和建议分配，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负责协调社区所作出的贡献，并提供资金帮助社区解决费用。这样做的目的之一是补偿社区成员在支持系统运作中产生的费用。

在启动之时，Zen将配有一个精通多个相关行业的DAO。当管理计划准备实施时，对于有些人而言这个DAO将成为受制于市场竞争中的轮廓编组，他们往往希望自己坚持自己的管理结构；广泛的社区将会做出这一决策。

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
松弛缓和
网页
博客 建议系
统 投票系统
二进制存储库

DAOs将提供以下支持： 帮助人们使用ZenCash或
其他系统功能 帮助安全节点操作者
排查节点奖励问题
排查投标系统问题 提供升级支
持 提供快速和最终问题的裁决
方法

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，但这将是没有限制的。负责人可以匿名，但不做硬性要求。实际上，公开身份的优点在于先前的专业成就和品格优点会自然地植入到Zen系统中。

这样做会引起争议，因此我们需要制定解决机制来有效并公正地做出裁决。在接下来的治理研发项目中将会探讨的一个计划，即建立司法和陪审制度。

7.2 建议提交与投票

每个DAO都有自己的结构，流程和优先级别，但它们有一个共同为工作、评估及奖励过程而设立的自由、开放的提交建议机制。我们没有理由去明确其发生的动因，因为它是理应发生的。这是一个全人类的开放社区，这里不应该有障碍阻挡参与。以下，是我们为初始的DAO提出的方法：

1. 每两个月投票一次。投票前两周提交投标截止日期。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天内以一致行使团队否决权（不建议做次决定）。

4. 在投票当日提出的建议可以以当地货币汇率计算相应会产生ZenCash（防止资金快速上涨导致项目遭到拒绝）。

5. 用代币进行投票。可在投票前1个月分发1440个代币。

6. 多数投票做出决策 > 720个代币持有者投赞成票。

7. 绝对多数投票做出决策 > 1080代币持有者投赞成票。

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：1 ZenCash
   (b) 31-60个代币：2 ZenCash
   (c) 61-90个代币：3 ZenCash
   (d) 以此类推，最多可花12 ZenCash

2. 240个代币——属于ZenCash项目开发者

通过提交、提出请求或其他合理的贡献措施给予奖励。

目标是授予软件和系统开发人员相关权利。.

3. 60个代币——用ZenCash进行交易

(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

5. 360个代币——安全节点

(a) 每40块奖励一个，直至360个分发完。

6. 120个代币——平分给DAO负责人

7. 240个代币——平分给核心团队

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、挖矿者、贸易商、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。

8.1 公开源代码中的伦理道德 虽然创始人希望我们一直将社区保持以Zen原则为中

心，但公开源代码会逐步形成
一套伦理问题。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。

8.2 Zen支持 Zen支持是指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，并将使Zen的技术最直观的，简易的参与到生态系统中。其次，Zen支持还将包括来自不同行业的使者，导师组成的贡献者网，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支持结构的设计旨在促进包容，协作和集体援助，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。

8.3 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如下所述。

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。其中将包括利益集团，他们都有在加密交易空间中不同的活动记录，这些人包括企业家，积极分子，开发商，大学，公司和不知情但充满好奇的个人。

通过我们的Zen代表项目（Zen Ambassador Program），有经验的用户，思想领袖和热情的社区成员将获得代表Zen的机会，需获得资源，资本，技术地向世界各地的人们表达我们的愿景，在去个人主动性下加入社区。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，全球青年可以获得密集编码和商业发展的教育培训，也会获得参与Zen集体的宝贵机会。这个项目涵盖将多方面，其中包括建立在Zen平台上为了DAO资助的创业公司而举行的全球青少年比赛，随机分配资源以支付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，并获得相关的启动创业加速器的特权，如有机会接触到例如成功的商业导师、营销和用户获取渠道，接触到参与开放源码的开发人员、直接渠道投资者和风险投资公司，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宪章的形式在全世界范围内改变他们对Zen技术、伦理道德、和（或）管理以及不断出现的项目的看法。Zen章程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详细介绍了Zen的起源、具体特点、差异和目标。

希望为团队创建Zen赞助的促销或教育活动，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章程加入的相关课程：编码法、企业家精神、去中心化的伦理学，区块链的基础等等。

业务计划数据库，法律文件，收入模式，用户获取策略等，以进一步开展业务发展计划的章节目标或努力改善社区。

通过Zen途径获得Zen贡献者和开发者的支持，建议，指导和帮助。 例如，在菲律宾适用的Zen章程，只有约30％的人可以获得金融服务，真正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FinTech国际共同开发项目中去。实际上，这个参与范围是可扩展的。扩大后的范围会很大程度地减少一些摩擦。这些摩擦可能因为历史阻碍了社区自主地发展其小规模经济而产生，也因阻碍其竞争力的增强而产生。

在21世纪，虚拟互动和沟通已成为了巨大的突破。这也将成为一个核心渠道，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。我们还将随机产生偶然事件用于特别保护一些Zen节点。其主题，内容和目的将根据Zen社区的喜好而有所不同。

我们的资源适用于我们的Zen社区，其中包括更多类的参与者和倡议，比传统加密项目下的利益相关者价值更高。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。

竞争性格局

“我们一直认为，随着时间的推移，许多公司往往会在做出微小进步的同时反复做同样的事情。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，你们要警惕暂停不前。 ——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加密货币适用范围扩大的竞争，和我们系统在生态系统区块链平台中的竞争。

ZenCash 与ZCash，Zclassic，Dash，Monero，ZCoin，比特币，ShadowCash，Boolberry，和一些其他私人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，我们直接与使用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。

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创业公司旨在为被剥夺权利的人提供服务。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空间做出贡献。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。

我们的价值主张是主动吸收将我们所认为的最佳典范，这些典范起初继承于零知识Zcash的实行，并通过zk-SNARKs进行保护。但我们采取了进一步关键步骤，通过端到端加密混淆整个网络，使消息在空间中最安全的基础设施中传递。重要的是，我们不打算转移与置换，因为我们已在结构上做好了准备。不仅仅是发展基础技术，更新和激活我们的系统，更是为了成为空间的创新者。

Zen正在建立一个以ZenCash作为价值符号或燃料交易的体系结构。就这点而言，我们还将与更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）。在这个领域里，Zen从比特币和ZCash继承的简单脚本语言保留了大量攻击向量的高安全性和弹性，但这限制了复杂代码执行的自由度，和具有增强的图灵完整脚本的平台的执行，这种情况类似于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，能够在越战略合作间跨链经营。

我们对加密货币体系的独特创新是我们竞争力强劲和变革性的治理模式，以在最佳去集中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，但其他项目已经进一步采取了各种投票机制。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竞争的情况下，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、尝试和犯错的创新而变。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。

我们将竞争视为健康成长进程的推动者，因此我们积极迎接最大化的竞争。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。

Zen的发展前景

虽然预测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，我们所创造的分权化、完全包容性、自愿、灵活的组织将比20世纪所流行的静止、集中、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远景。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。

通过我们早期的组织执行路线图，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挑战，但是灵活性和持续的平合作将克服这些似乎无法逾越的问题。

我们足够幸运，生活在一个有着不可置信的技术和创意的创新时代。我们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，但是他们中有许多人的姓名不被人所知。因为他们是一个巨大的群体，他们的贡献是基础而重要的。

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 Du eld, Kyle Hagan. (2014) Darkcoin: Peer-to-Peer Crypto Currency with Anonymous Blockchain Transactions and an Improved Proof-of-Work System.

[4] David Fi eld, 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 Speci cation 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 Re-store the Environment, Enrich the Poor, Cure the Sick, and Liberate Humanity from Politicians. Free Press.

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