

zencash

系统更新技术规范

Zen应用平台： 多层次节点系统及侧链 以实现网络去中心化

2018年四月

Pier Stabilini, Robert Viglione, and Alberto Garoffolo

介绍

ZenCash安全节点系统是一个独特的有偿区块链网络，具备增强化的客户端到节点及节点到节点的加密功能。该系统的设计目的旨在于迅速、大规模地令区块链网络去中心化，提供无与伦比的抗审查能力和网络容量，并为高性能的隐私保护平台奠定基础。在运行该系统仅仅不到三个月的时间内，我们的网络在节点数量上已经可以与比特币相媲美。尽管取得了巨大的成功，但这仅仅只是一个开始，我们的这个次时代系统将为节点跟踪和支付提供重大改进，更重要的是，为综合性应用平台奠定基础。

技术层面的改进包括：

- 创建一类新型节点，称为超级节点，它们具有更高的 ZEN 持币（500 枚 ZEN）要求、算力及存储空间要求。
- 将逻辑从链下服务器群集迁移到侧链上，这些侧链由新的超级节点们维护。多层侧链也将使 ZenCash 能够支持 ZenPub、零延迟支付（InstantZen）、ZenGrid（算力出租服务）和ZenXchange（建立在我们网络上的去中心化交易所）等多种应用，此处仅举几例。
- 提供一个完全去中心化的节点跟踪系统，其节点状态由其连接的对等节点中继转发，并且所有的安全节点信息都通过核心协议被接收。

经济层面的变化包括：

- 节点运行者将获得出块奖励的 20%，这与先前的 3.5% 相比提升不少。奖励将对半分配，即安全节点运行者获得 10%，超级节点运行者也获得 10%
- 出块奖励的 10% 将划入储备金，这与先前的 8.5% 相比有所提升。
- 矿工将获得出块奖励的 70%，折与先前的 88% 相比有所下降。

ZENCASH 概况

ZenCash是一个注重隐私保护的区块链系统，基于零知识证明密码学及修改后的中本聪共识。该系统远远超出了传统加密货币的定义，它是专为能够打造成一个初创企业之国而设计，是专为资金、媒体和信息打造的完全点对点的经济系统。

该项目始于其核心产品 ZenCash，这是一种可以选择保护隐私的程度或透明度的加密货币。用户可以在完全私密的地址类型或像比特币这样的匿名地址之间进行选择。除了交易隐私之外，该系统还将 SSL / TLS 引入到用于客户端到节点及节点到节点加密的协议中，以进一步保护用户数据和连接。

中本聪共识通过防止双花问题(double spending)以及调整矿工奖励机制（让他们诚实地参与

区块创建) 来保证数字稀缺性。但是, 该系统并未向其他利益相关者(如全节点运行者) 提供此类奖励措施。我们的创新是直接从出块奖励中支付全节点运行者报酬, 但却要求这些节点运行者具有有效的证书、满足最低的计算能力以及最小的正常运行时间要求。这创建了一个更高质量和更可靠的节点网络, 但原始系统的弱点在于, 所有的逻辑都放在链下服务器集群及外部数据库上托管。我们的下一步改进是将所有的逻辑放在链上, 并使整个过程自动化。

超级节点引入了侧链和平台应用。这是对原始系统的重要改进, 使得我们的项目不再仅仅只是简单的加密货币。

安全节点

ZenCash 安全节点系统 旨在大规模地令我们的网络去中心化, 以便该项目可以在全球司法辖区内具备反审查力。全节点运行者如果持有有效 SSL / TLS 证书、在透明地址(t 地址) 中存放至少 42 枚 ZEN, 并成功响应至少 92% 的发送到受保护地址(z 地址) 的挑战, 则可分到挖矿奖励的 3.5%。这些要求都没有随本次系统更新而改变, 但我们在节点正常运行时间的衡量标准上引入了一个改进, 即基于实际网络对等连接而不是 websocket 连接。

当前的系统配置将运行跟踪及支付服务托管在全球某些地区的链下专用服务器集群上。这对于原始系统来说已经足够了, 而将所有的逻辑迁移至链上则是新系统的一个重要改进-这对于实现真正的抗审查和网络韧性, 并引入可验证和审计的信息集用于计算奖励这两方面来说十分重要。本次更新将所有内容写进协议内, 并利用由超级节点管理的侧链来跟踪安全节点, 安排节点报酬支付, 并与挖矿节点协调报酬的自动分配。

总而言之, 新版安全节点将提供许多改进, 其中包括:

- 在核心代码中实现协议层的所有逻辑, 而不是在一个分离的代码库中。
提供一个完全去中心化的节点跟踪系统, 节点状态由其连接的对等节点中继转发, 并且
- 所有的安全节点信息都通过核心协议被接收。

安全节点的大部分要求将保持不变:

- 在系统上维护整个 ZenCash 区块链
- 向 ZenCash 节点软件提供有效的 SSL 证书, 以用于与其他节点和钱包进行通信。
- 将至少 42 枚 ZenCash 存放在一个 t 地址中以获得持币收益。
- 监视所有网络信息以获得挑战信息。
- 通过识别安全节点的信息来响应挑战。
- 每日须达到 92% 的正常运行时间。



即将引入的变化:

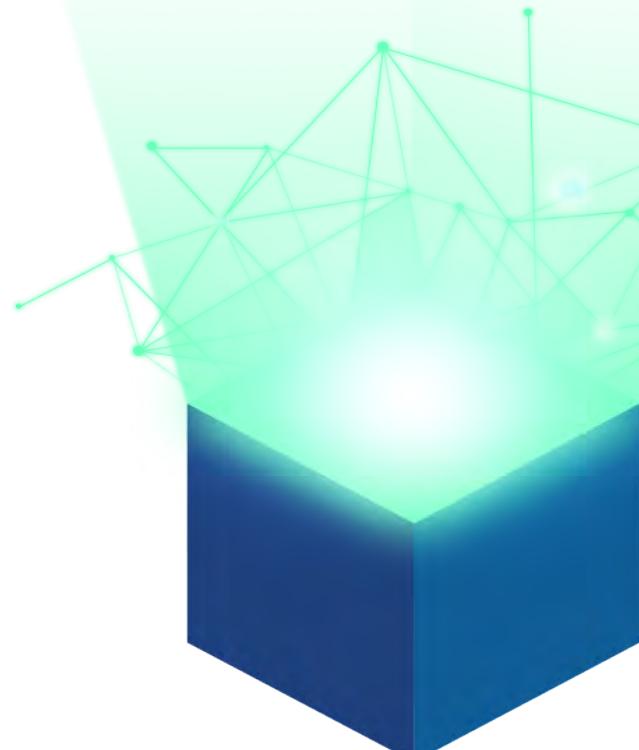
- 依赖新版 zk-snark 的全新挑战机制的内容要求是 1.7Gb。此改动正于 2018 年 3 月发布在测试网络上的前期软件更新中被引入，并计划于 2018 年 5 月在主网上正式发布。
- 正常运行时间根据实际网络对等连接和区块链同步进行计算。
- 安全节点奖励将提升至出块奖励的 10%。

在协议层，信息处理程序将支持必要的消息以完成下列功能:

- 将安全节点信息和状态穿播至全网。
- 验证一个特定交易、一组交易或某个特定区块的哈希值以检查节点是否同步。
- 执行挑战或其他检查来验证节点要求是否得到满足。
- 所有其他必要的信息已被写进协议层。

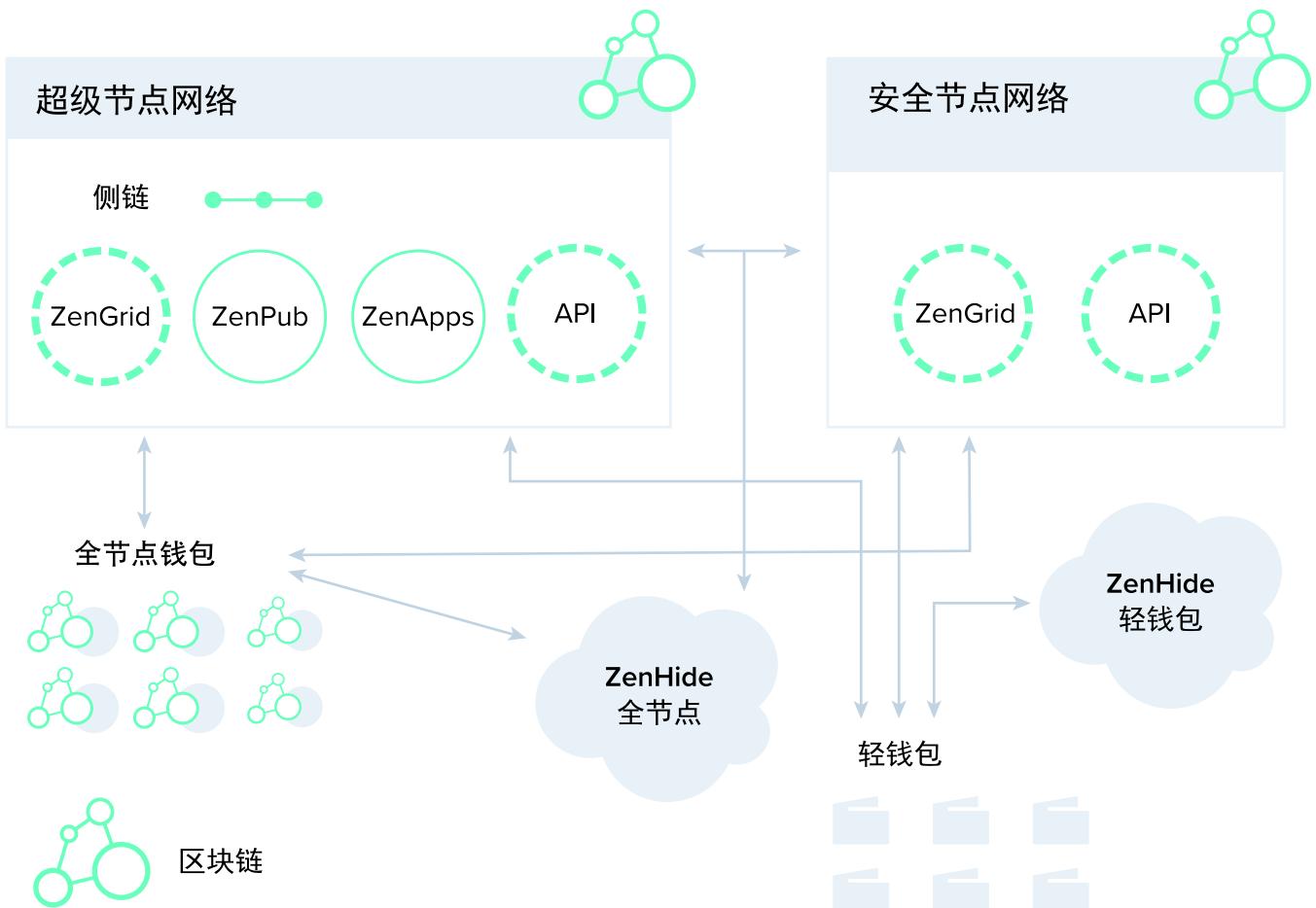
超级节点与侧链

我们系统首批与众不同的主要特性之一是推出了具有增强的点对点加密的有偿节点网络，我们称之为安全节点。ZenCash 网络在发布该系统后的仅仅四个月内便获得了超过 9,000 个安全节点，比预期的要多出3倍。网络上的这些节点由足够高质量的系统组成，以满足最低要求：其中包括拥有有效的 SSL 证书，这与当前市面上其他区块链相比是一个极大的进步。接下来的一个阶段是创建一类具有更高要求的特殊节点，我们称之为超级节点。超级节点将比安全节点更强大，并将肩负管理关键网络和系统功能的职责，例如在侧链上运行多种服务、跟踪和测量安全节点正常运行时间、并为矿工安排节点报酬支付时间表。



超级节点所带来的两大改进是将跟踪和支付活动迁移至链上，或协议层内，这与当前系统相比是一个重大改进，因为目前这些功能在外部服务器集群上执行；而侧链的引入将 ZenCash 系统从一个纯粹的加密货币升华至可以构建无数服务的平台。这样，该系统的价值主张就不仅仅是实现货币功能，还会包括利用到所有未来服务，这些服务将被铺设在我们的基础设施上。目前正在规划中的此类服务的一小部分包括分布式文件存储系统（ZenPub）、安全即时通信系统（ZenChat），类似 AWS 的 Lambda 函数的算力出租系统（ZenGrid）、零延迟支付（InstantZen）以及一个去中心化交易所（ZenXchange），里面有名为 ZenUSD（USDZ）的完全抵押的、价格稳定的资产。

ZEN网络



节点报酬支付管理

超级节点网络将支持多层侧链。其中一层将用于存储有关安全节点状态和超级节点状态的所有信息。具体来说，超级节点网络将跟踪侧链上安全节点和其他超级节点的状态。该网络将使用共识机制来检验和确认所有必要的跟踪信息。

这种排队过程可按如下步骤运作：

- 每隔 n 个区块，超级节点将读取侧链以处理可获报酬的节点并将其移入队列中。
- 然后，所有的超级节点应就队列中的每个元素达成共识。
- 矿工节点将从队列（一个子集）中抽取元素，并在一个特定的 coinbase 交易中（矿工和社区的标准 coinbase 奖励除外）向节点进行支付，已获得报酬的节点从队列中被移除。

已获得报酬的节点将从队列中被移除，并将由超级节点再次插入到队列中，以便进行下一轮报酬支付。

侧链管理和系统要求

超级节点将支持多层次的侧链，这将为我们系统的平台化奠定基础。

这些侧链将用于各种应用，并将通过通用接口来连接，以包含 RPC 方法。第一个实施将用于从 Insight API 中查询节点状态。如上一节所述，多层侧链可以使 ZenCash 支持多种应用。此外，ZenCash 将能够利用侧链整合第三方技术，例如 FlowCrypt（用于 Gmail 的 PGP 扩展），以将整个公钥集存储到侧链中。值得注意的是，出于安全原因，这套应用最初只会局限于内部开发，但我们未来的目标是向外部 dApp（去中心化应用）开发者开放我们的平台，以便任何人都可以直接为生态系统做出贡献。

这是对系统功能和生态系统价值主张的重大改进。为支持该功能，超级节点的要求会更高：

- 在一个 t-地址上至少存放 500 枚 ZEN 以获得持币收益。
 - 多核 CPU。
 - 8GB 以上的内存。
 - 100GB 以上的硬盘空间。
- 每天至少达到 96% 的节点正常运行时间。

奖励、调整及网络目标

ZenCash 生态系统的一个主要方面是：我们希望最大程度地实现去中心化以对抗审查。我们知道，通过设置明显更高的持币要求 - 从 42 枚 ZEN 到 500 枚 ZEN，我们面临着超级节点架构过度中心化的风险。避免过度中心化的一种方法是增加奖励池以激励大家创建更多节点。这是将节点运行者的报酬从挖矿奖励的 3.5% 到 20% 的主要原因，其中 10% 用于安全节点运行者，另外 10% 用于超级节点运行者。

分离奖励池应带来联合均衡，即令网络增长到边际成本等于边际收益的临界点。超级节点的边际成本会高得多，因此我们预计它们数量会少一些，但它们的收入流将独立于安全节点奖励池，因此一个细分领域（超级节点）的增长不应该会过度蚕食另一个细分领域（安全节点）的收入状态。我们的目标数量分别是 2000–2,500 个超级节点和 20,000–25,000 个安全节点。如将来与该目标出现重大偏离，则可能不会有后续的奖励或持币收益调整。

实施时间表

搭载超级节点的该应用系统的全面实施预计将于 2018 年第四季度启动，第三季度末发布可用于测试的原型。我们网络的建设将很快开始。出块奖励调整将在下一次硬分叉系统升级时

执行，其计划在 4 月中旬发布到测试网络上，并在 5 月底发布到主网上。

为鼓励超级节点网络尽快顺利扩展，我们推出如下计划：

- 在 5 月底下一次硬分叉来临时，启动超级节点持币收益系统。
- 未来的超级节点运行者需要注册一个 t 地址，并在上面存放至少 500 个 ZEN。
- 超级节点运行者将运行安全节点软件的一个修改版本。
- 出块奖励的 10% 将累积到专用的超级节点多重签名地址。
- 超级节点运行者将得到类似于当前安全节点系统的报酬，直到第四季度产品级软件发布。

本机制提供了部分奖励，以便尽早开始筹备超级节点，但随后还要在系统正式开始运行时跟进设置好节点。由于预期数量的超级节点将需要 100 万到 125 万枚 ZEN 放入持币地址，所以最好提前启动这个积累过程，并延长运行一段时间，而不是在第四季度突然启动。我们相信这种混合奖励机制既能激励早期积累，又能在系统上线时跟进设置好超级节点。

总结

我们在本白皮书中提出了多层次的重要系统升级。超级节点系统将把安全节点跟踪和支付活动迁移至链上，并实现自动化流程，以达到更高的效率并提升可靠性。系统的经济机制将发生变化，极大地激励用户设立更多安全节点和超级节点。报酬数额增加近 3 倍的措施将大大增加运行节点的数量，引入超级节点可提升构成网络的系统质量。然而，最值得注意的公告是，这个庞大且仍在不断增长的网络（可能是业内最大的网络）将转变为分布式应用聚集的平台，通过多层侧链实现。已经提上我们开发日程的每个应用都会为社区带来重大效用，但这仅仅只是一个起点。我们未来的目标是向外部 dApp（去中心化应用）开发者开放我们的平台，以便世界上任何人都可以为生态系统做出贡献。我们的使命始终是整合社会，减少人为冲突，让世界变得更加美好。这些系统更新将会带来一个更加强大的网络，以此为起点开始真正的趣味创新旅程！

参考文献：

- [1] -<https://github.com/ZencashOfficial/>
- [2] -<https://zencash.com/>
- [3] -<https://securenodes.eu.zensystem.io/>

