VELES

白皮书

Veles: 开放的分布式VPN和匿名网络生态系统

2018.12.09
1.01 版

作者**:**
@AltcoinBaggins
@mdfkbtc
翻译**:**
@Tigermumu

摘要：

Veles是一项开源软件项目，旨在帮助互联网社区提高信息访问自由度，防止互联网监察，并改进互联网通信的匿名性。我们相信中本聪（Satoshi Nakamoto）引入的区块链技术，并被许多其他开发人员（例如，引入主节点系统（masternode）的Dash团队）进一步优化与推进后，可以帮助我们构建分布更加公平，可靠和稳定的网络。用于目前基于洋葱网络提供匿名连接的开源技术建立在仅仅由几名志愿者搭建起的简单网络概念之上。区块链背后的主要思想之一是利用博弈论模型构建自我支持网络，参与者因受到经济激励而支持它。我们相信，将这种新技术和经济概念的优点与数千名密码极客已经建立的网络通信匿名技术相结合，一定可以实现Veles项目的愿景，从而促进互联网社区的进步。

1. 介绍

比特币和区块链背后的假设和技术已经自证有效性超过10年，也见证了它不断被发现以及不断被解决的各种技术问题。Veles遵循着行业内最出色的实践项目，凭借精心的项目管理和开发过程，Veles生态系统可以提供安全的点对点区块链网络和加密货币，抵御当前常见的威胁，如51％攻击或者是未来可预见的量子计算威胁，同时以最低的费用确保快速交易。Veles加密货币是整个生态系统的基石，它为网络参与者提供激励并支持生态系统中的微观经济。

为了防止监察并改善互联网上的通信匿名性，Veles项目开发的主要关注领域之一是采用隧道协议和虚拟专用网络（VPN）技术，以及SSL/TLS，公钥方案和数字证书来创建安全的点对点连接。

2. 共识改进方案

我们改进区块链功能的基本策略是基于升级奖励系统，安全性和工作量证明概念的实用性。我们用以下技术实现它：使用多种算法结合的动态区块奖励机制和insta-mine保护(防止高算力切入时大量出块)，Veles升级了矿工奖励系统和抵御51％攻击的能力。此升级还最大限度地减少了对投机性挖矿的奖励，防止出现恶意砸盘并做空经济系统的情况。

动态区块奖励会根据每个算法的哈希值单独计算。例如：如果X11算法为200GH/S，而Scrypt为5MH/S，则X11算法中的出块奖励为大约0.2 VLS，而Scrypt的出块奖励为0.003 VLS。因此，不可能出现单一算法获得大量出块奖励的情况。

多算法挖矿机制为大量矿工提供了挖矿机会，我们认为这可以改善网络分布性和区块奖励的分配。这使GPU和ASIC矿工都能够在Veles网络中找到自己的位置。每个算法的奖励分配在整个网络中是一致的，例如。如果X11算法累积了200 GH/s的哈希值，则奖励将与30 MH/s的Lyra2z算法相当。而且，如果攻击者要成功实现51％的攻击，则必须控制每个算法51％的哈希值。另外，Insta-mine保护工作的效果是：如果单个算法哈希值突然增加超过50％，则该算法的下一个区块的挖矿难度将大大增加，并且随着后续区块的产生而缓慢降低。这一机制同时还可以消除可预见性的出块时间分歧。

多算法系统其中之一的组成部分是，每种算法重新计算并单独改变难度的方式。难度设置由死锁保护控制，它能够应对出块冻结问题并有效地重新计算由于哈希值的突变而引起的难度变化。这使得快速投机性挖矿变得异常困难，因为前序交易需要首先被确认。

3. 匿名性，隧道协议和 **VPN**

虚拟专用网络（VPN）技术使 Internet 用户能够绕过地理限制和官方监察，连接到代理服务器以保护个人身份和位置，从而实现在 Internet 上保持匿名性。但是，一些 Internet 网站限制主流 VPN 的解决方案，以限制某地理位置的用户访问。尽管一些 VPN 提供商正在寻找解决这些问题的方法，但它们并不一定能为所有互联网用户提供永久可靠的解决方案。

有几种成功的策略来解决这些限制，并改善通信的匿名性。其中一种有效的解决方案是使用多层转接的洋葱路由。为了在典型的洋葱网络中传输信息，发起者从列表中选择一组节点。所选择的节点被安排在称为链或环的路径中，通过该路径传输消息。为了保持发送者的匿名性，节点环路中的任何独立节点都不能判断它之前的节点是发起者还是中继点。同样，环路中也没有节点能够知晓其中到底有多少其他节点，只有最终节点（退出节点）能够确定其自身在链中的位置。

目前像洋葱浏览器这样的自发性网络协议可能仍然存在一些弱点，我们认为可以通过实施基于区块链的 Masternode（主节点）技术来改善这种弱点，区块链的理论模型可构建自支撑和自我调节的网络，使 VPN 和洋葱路由服务可以以更公平，强大，安全和可靠的方式提供。

Masternodes（主节点）的概念使用辅助网络扩展了区块链，称为 Masternode（主节点）网络。这些节点将具有高可用性并为网络提供所需的服务级别并参与通证质押，以此获得 Veles 代币奖励。这一机制可以为网络提供不限量的附加服务。另一方面，抵押代币和高可用性的要求将阻止不良行为者参与。Masatode（主节点）网络已经作为一种概念证明在 Dash 白皮书中引入，它是第一个实现包括 PrivateSend 和 InstantSend 功能的概念。

Veles 网络将进一步构建 Dash 引入的 Proof-Of-Service（服务即证明）概念和 Masternode（主节点）网络系统，将其与 OpenVPN 等强大的开源技术集成，OpenVPN 是一个全功能的开源 SSL VPN 服务器和客户端软件库。得到众多操作系统平台的支持，包括 iPhone，Android，Windows，Linux，MacOSX 平台。OpenVPN 安全模型基于 SSL，这是通过互联网进行安全通信的行业标准。OpenVPN 使用 SSL/TLS 协议实现 OSI 第 2 层或第 3 层安全网络扩展，支持基于数字客户端证书的灵活客户端身份验证方法，并搭配应用旨在防御被动和主动攻击的工业级安全模型。

Veles 的 Masternodes（主节点）系统也引入了 II. Tier Masternode 网络以提供节点出口的功能。这些节点仅需要提供 I. Tier Masternode 的一半质押额度和更少的计算能力以及存储器资源需求，仅提

供网络带宽，用来实现多转接路由器或出口节点功能，以构建类似于洋葱网络的环路节点。这些节点可以在多个设备上运行，包括那些低配置硬件设备，如 Raspberry Pi。愿意提高其通信匿名程度的用户将能够按需选择转接层数来完成路由。

为了确保服务的最佳性能，速度，公平性以及阻止类似于 DDoS 的攻击，每个 VPN 用户需要用 Veles 网络的加密货币支付低廉的费用才能获得对 VPN 服务的访问权限，以便网络不被滥用。为了全面提高匿名性，支付交易不会直接发送给节点运营商，而是发送到“燃烧地址”上。节点运营商将定期收到该地址分配的公平奖励，以便实现一致性的服务级别，而与用户所支付的费用无关。我们的目标是尽可能降低此费用，以维持其反垃圾邮件攻击和防止被滥用功能。

这种策略还可以帮助防止网络中心化，因为网络的机制会阻止参与者建立少数的强大节点，反而鼓励他们增加节点的数量，从而实现地理位置路由的多样性和生态系统的分散化。消耗 VLS 来使用 VPN 的计划也将通过降低 VLS 的释放量和减少流通的 VLS 数量，来帮助微观经济，从而促使 Veles 加密货币实现长期稳定增长的价值。

4. 愿景

我们的愿景是构建项目并引导它成功实现自我激励，自我支持和自治的分布式网络和生态系统，为互联网用户提供强大，可靠和安全的 VPN 和匿名服务，利用最新技术和最佳实践经验，建立受社区支配的开放式生态系统，我们认为这可能比前面提到的传统的自愿组织方式或专门的商业性解决方案更可靠有效。本白皮书仅用于　　白皮书中　展示该项目的方向并解释我们的目标。 Veles 团队的目标是引导和保护 Veles 生态系统开发和管理所涉及的所有流程，直到网络足够成熟，并在开放治理，项目管理和开发流程进入最后阶段之时，在智能合约和算法辅助下，将生态系统最终完全转交于社区之手。