VELES

whitepaper

Veles: Open decentralized VPN and anonymous networking ecosystem

Dec 9 2018,
Version 1.01

Authors:
@AltcoinBaggins
@mdfkbtc

Abstract
Veles is open-source software project that aims to help the Internet community to improve freedom of access to information, to prevent Internet censorship, and to improve anonymity of the communications on the Internet. We believe that blockchain technology, introduced by Satoshi Nakamoto and further advanced by many other developers, such as the Dash team which introduced masternode system, can help us to build more fairly distributed, reliable and robust networks. Existing open-source technologies for providing anonymous connection based on onion-networking are build upon concept of simple volunteer networks. One of the main ideas behind blockchain is using game theory models to build self-supporting networks, where participants are economically incentivized to support it. We belive that merging the advantages of this new technological and economical concepts with years battle-proofed foundations for anonymization of the communications over networks already laid by thousands of cypherpunks and hackers could be the right way to achieve the vision of Veles project and to move the technology that helps the Internet community another little step forward.

1. INTRODUCTION

The hypothesis and the technology behind Bitcoin and the blockchain has already been proving its validity for more than 10 years and even thought it has faced many challenges, they keep getting solved at a rapid pace. By following industry's best practices, careful project management and development proccesses, the Veles ecosystem can provide secure peer-to-peer blockchain and cryptocurrency, resistant to current common threats like 51% attacks or future threats such as the one posed by quantum computing, while ensuring fast transactions with minimal fees. To provide the network incentivisation and support it's micro-economy, Veles cryptocurrency is the cornerstone of the Veles ecosystem.

To prevent censorship and improve anonymity of communication on the Internet, one of the main focus areas in the development of Veles project is employing tunneling protocols and virtual private network (VPN) techniques to create secure point-to-point or connections, utilizing SSL/TLS, public-key scheme and digital certificates.

2. CONSENSUS IMPROVEMENTS

Our basic strategy on improving blockchain functionality is based on upgrading the reward system, security and practical utility of the Proof-of-Work concept. We have attained it using the following technologies:
Using multiple algorithms combined with dynamic block rewards and insta-mine protection, Veles upgraded miner reward system and the ability to sustain 51% attacks. This upgrade also minimizes attempts towards speculative mining and prevents to reward miners with "cheap coins" in such situations.

Dynamic block rewards are calculated individually on the basis of each algorithm's hashrate. Eg. if the X11 algorithm is at 200 GH/s while Scrypt is at 5 MH/s, the rewards in the X11 blocks will be ca. 0.2 VLS, while Scrypt will be rewarding miners with ca. 0.003 VLS per block. It is therefore impossible to favour a single algorithm compared to other less used ones.

Multi-algorithmic mining gives a large number of miners the opportunity to mine, which in our opinion improves the network decentralization and reward distribution. This allows both GPU and ASIC miners to join the Veles network in a harmony.
The reward distribution per algorithm is consistent across the entire network, eg. if X11 accumulated a hashrate of 200 GH/s, the rewards will be comparable to Lyra2z at 30 MH/s. To successfully do a 51% attack, an attacker would have to control 51% of hashrate on each algorithm.
Insta-mine protection works as follows: if a single algorithm hashrate will suddenly increase by more than 50%, the difficulty of mining will be substantially increased for several next blocks, with a slow difficulty bleed off. This eliminates speculative block time warps.
An integral part of this multi-algo system is the way in which each algorithm recalculates and individually changes a difficulty. The difficulty settings are controlled by a dead-lock protection, which protects against freezing and effectively recalculates the difficulty both with sudden increases and drops in hashrate. This makes quick speculative mining of coins difficult as previous transactions are required to be confirmed first.

3. ANONYMIZATION, TUNNELING AND VPN

A virtual private network (VPN) technology VPN enables Internet users to circumvent geo-restrictions and censorship, or to connect to proxy servers to protect personal identity and location to stay anonymous on the Internet. However, some Internet sites block access to popular VPN solutions to prevent the circumvention of their geo-restrictions. Even though some commercial VPN providers are looking for a ways to get around this issues, they don't necessarily provide permanent and reliable solutions to all the Internet users.

There are several successful strategies to get around these restrictions and to improve the anonymity of the communication. One of the efficient solutions is using multi-hop onion routing. To transfer the information in classic onion network, the originator selects a set of nodes from a list. The chosen nodes are arranged into a path, called a chain or circuit, through which the message will be transmitted. To preserve the anonymity of the sender, no node in the circuit is able to tell whether the node before it is the originator or another intermediary like itself. Likewise, no node in the circuit is able to tell how many other nodes are in the circuit and only the final node, the exit node, is able to determine its own location in the chain.

Current voluntary networks such as Tor may still suffer from several weaknesses which we believe could be improved by implementing masternode technology based on blockchain, which draws from game theory models to build self-supporting and self-regulating networks, where VPN and onion routing services could be provided in a fair, very robust, safe and reliable manner.

The concept of masternodes extends the blockchain with secondary network, called the masternode network. These nodes will have high availability and provide a required level of service to the network and have a bond of collateral to participate, in order earn their payment in Veles cryptocurrency. These can provide any number of extra services to the network. On the other hand, the collateral and the requirement for a high availability will discourage bad actors to participate. The concept of Masternode Network has been introduced in the Dash Whitepaper, and as a proof-of-concept, it's first implementation included PrivateSend and InstantSend.

Veles network will further build on the Proof-Of-Service concept and masternode network system introduced by Dash by integrating it with robust open-source technologies such as OpenVPN, which is a full-featured open source SSL VPN server and client software / library that is supported by a wide range of clients, including iPhone, Android, Windows, Linux, FreeBSD or macOS platforms. The OpenVPN security model is based on SSL, the industry standard for secure communications via the internet. OpenVPN implements OSI layer 2 or 3 secure network extension using the SSL/TLS protocol, supports flexible client authentication methods based on digital client certificates and uses an industrial-strength security model designed to protect against both passive and active attacks.

Veles masternodes system also introduces II. Tier masternode network to provide function of exit nodes. These nodes will require only half of the collateral of the full I. Tier masternode but will also require substantially less computing power and memory resources, only providing network bandwidth and functioning as multi-hop routers or exit nodes to enable onion-like circuits. These nodes could be run on number of devices including those with low resources such as Raspberry Pi. Users willing to improve degree of anonymity of their communications will be able to choose any required number of so-called hops to route their traffic through.

To ensure the best availability, speed, fairness of the service and to discourage DDoS-like attacks each VPN user will need to pay a low and affordable fee in Veles cryptocurrency in order to obtain an access to the VPN service, so that the network cannot be easily misused. For sufficient anonymity of a payment for the VPN service the transaction won’t be sent directly to the node operators but rather to the so-called burn address. The node operators regularly receive their fair rewards for providing the required level of service in a consistent manner independently of fees paid by the users. Our goal is to keep this fee as low as possible just to maintain it’s anti-spam and counter-misuse role.

This strategy can also help to prevent centralization as the network will discourage participants to build fewer powerful nodes but will rather encourage them to increase the number of nodes enabling grater diversity and decentralization of the ecosystem. The plan of burning VLS fees for VPN use will also help the micro-economy by either decreasing emission rate of VLS or even possibly decreasing number VLS in the circulation, helping the cryptocurrency to better keep it's value over time.

4. THE VISION

Our vision is to build and bootstrap successful self-incentivized, self-supporting and self-governing decentralized network and ecosystem providing robust, reliable and safe VPN and anonymization services to the Internet users, taking advantage of up-to-date technology and best-practices, to build open ecosystem governed by the community resistant to the censorship, which we believe could be far more efficient than conventional voluntary or proprietary solutions mentioned earlier. This whitepaper is intended to only show direction of this project and to explain our goals. The purpose of the Veles team is to bootstrap and guard all the processes involved in the development and management of the Veles ecosystem until the network will be mature enough and will reach the final stage when the right open-governance, project management and development processes will be well-established and tested to the degree that the ecosystem could be ultimately put solely into the hands of the community, guided by smart-contracts and algorithms.