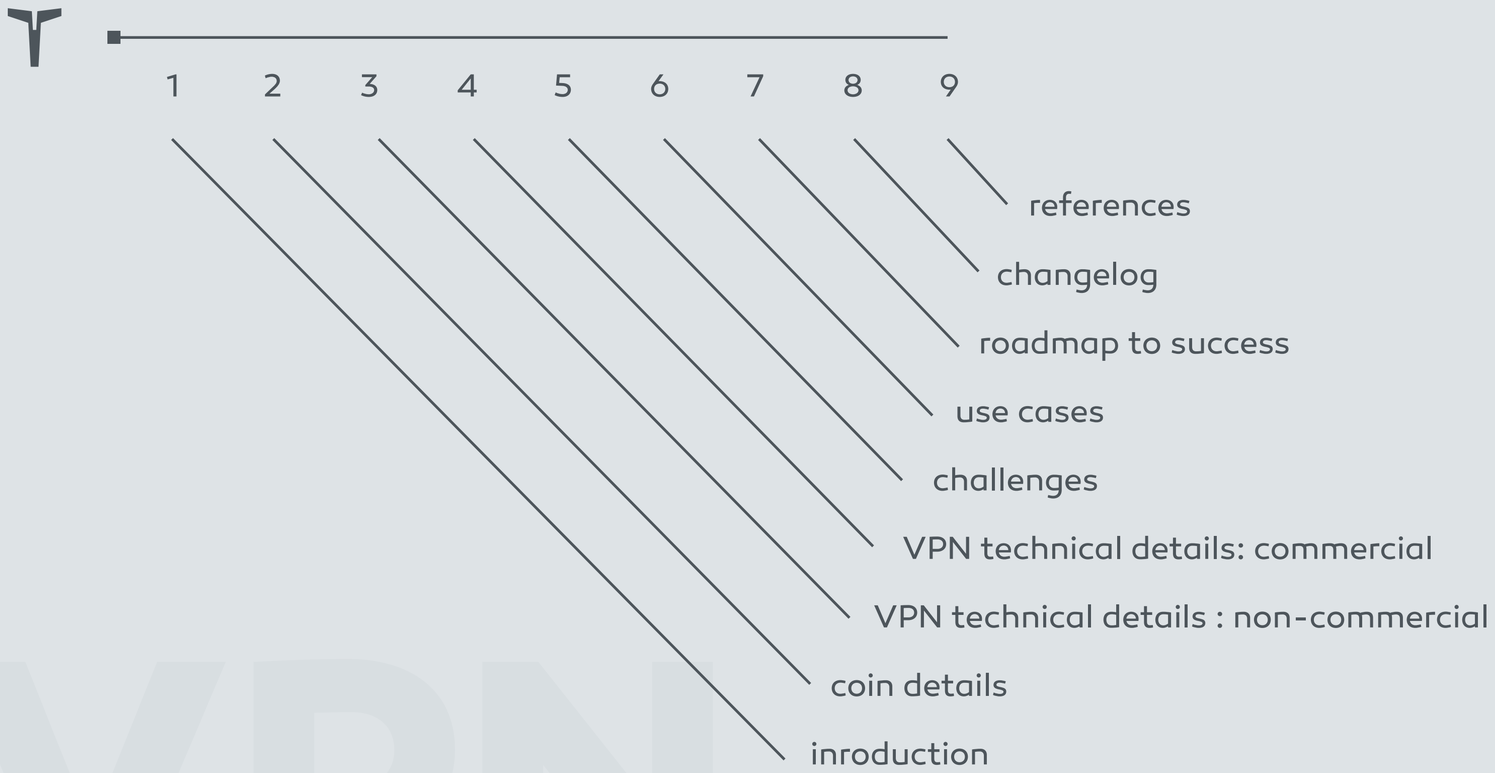
VPN WHITEPAPER

Lethean Coin
Version 2.0

Lethean Coin Team
1st September 2018



Click

the numbers

to navigate throughout

the document, and the logo to

return to this page.

Introduction

Today, privacy and security on the Internet are paramount concerns for users at all levels. In days past, such matters concerned only the technologically elite and organizations with enterprise-level security requirements. The landscape of internet security has shifted, and everyday users now recognize the threats posed by malware and counterparties. Security necessity for end-users has progressed beyond simple antivirus software to now demand protection and security of network traffic.

Lethean (LTHN) is the moniker for both a suite of privacy products and the cryptocurrency backing the store and transfer of value for said products. Lethean addresses the growing and persistent need for secure internet usage by establishing a peer-to-peer, decentralized, blockchain driven, anonymous virtual private network (VPN). Lethean strives to fulfill a mission of internet freedom and equitability, and a decentralized VPN network is an imperative step toward this goal. To meet this goal, the Lethean network will offer two mechanisms for VPN connectivity: full network VPN (utilizing OpenVPN technology) and a browser extension to secure web browsing and web services. True to classic cryptocurrency ideals and values, the Lethean network will allow anyone to act as an exit node for peer-to-peer (P2P) VPN tunneled connections. In effect, a decentralized VPN is created. The Lethean network will also serve as a centralized marketplace for commercial VPN operators to advertise and establish VPN connections.

Virtual private networks (VPNs) exist to obscure and secure traffic between endpoints. By using cryptographically secure tunnels for network data, internet traffic remains impervious to wiretapping and eavesdropping. The protections offered by VPN usage allow consumers to access the internet without the risk of leaking data to attackers monitoring network traffic, without restriction by corporations or governments, and without geographic limitation. Economic projections for VPN markets are favorable for Lethean. For example, the global SSL VPN market is projected to grow 7.5% annually [CAGR] and increase from $3.08 billion in value to $5.33 billion from 2017 to 2023 [1]. Mobile VPN demand is projected to grow at a staggering 21.1% from 2017 to 2022 [2].

A pillar of use for virtual private networks is anonymity. Lethean will address the crucial need for anonymity not only by utilizing encrypted peer-to-peer tunnels for data, removing the possibility of nefarious individuals analyzing or monitoring traffic, but also by means of an anonymized mechanism of payment. As a digital currency, Lethean is capable of anonymizing senders and receivers unlike conventional Bitcoin-based cryptocurrencies.

This is due to use of the CryptoNote algorithm which utilizes ring signatures to mix transactions among multiple receivers to create anonymity [3].

While many VPN services exist today and are sold under the premise of allowing anonymous web browsing, these advertisements tend to foster a false sense of security. Users are often easily traced back to their activity on VPNs by means of payment used to acquire the service. Some modern VPN companies have improved upon this flaw by offering payment via Bitcoin rather than conventional credit card or usual online payment processors. However, Bitcoin also offers a false sense of security and anonymity. It is known that extensive forensic monitoring and analysis operations are in place for Bitcoin, and payments can be readily traced back to senders [4].

In addition, most VPN providers track users' habits and keep detailed logs of every action. Lethean addresses these shortcomings of the classic VPN delivery model by combining a decentralized network with anonymous, untraceable payments, and abstain from logging user data.

While commercial VPN providers and services abound, end users lack a reliable or clear method of comparing services and prices. Lethean will allow these providers to list the prices and details of their service offerings in one convenient marketplace, side-by-side with Lethean P2P VPN exit nodes. In simple terms, Lethean wallets and products will be to VPN services what eBay or Amazon are to general goods: multiple sellers from multiple regions will list their proxy and VPN services, allowing end-users the ability to freely select the exit node which makes the most sense to them considering cost, bandwidth, speed and location.

Significant attention has been devoted in the conceptualization and development of the Lethean network and VPN to avoid affiliation with nefarious end users. As VPNs only offer anonymity as much as an IP address is anonymous, it is conceivable that some individuals seek to use such services to avoid association with or conviction for criminal activities. The Lethean product design philosophy emphasizes our products and network primarily as a tool for accessibility, net neutrality, and anti-censorship, rather than as a tool for nefarious users to utilize as a means to circumvent law enforcement.

Lethean details

Lethean exists foundationally as a cryptocurrency, based upon CryptoNote to allow for anonymous transactions. Ring signatures are used to prove that a transaction occurred between parties but without allowing determination of who truly owns or received the coins in question, limiting analysis of the blockchain. The same technology is used by Monero (XMR). As with most cryptocurrencies, Lethean coins are created by mining blocks of the blockchain, using CryptoNight as the proof-of-work algorithm. However, unlike classic Bitcoin-derived cryptocurrencies, Lethean can be mined efficiently with processor (CPU) power alone rather than relying on expensive video card (GPU) setups. The proof-of-work mechanism to create Lethean coins emphasizes the egalitarian philosophy of the product.

The Lethean team chose to emphasize accessibility of the coin and product by foregoing an initial coin offering (ICO) and instead allowing the community to establish, maintain and determine the value of the coin. Given the absence of an up-front funding opportunity provided by an ICO, the Lethean team created a 10% premine to be shared among core members and a 5% premine to be used for bounty rewards.

Lethean is an accessible cryptocurrency that is freely mineable by anyone with a computer, and will produce declining block rewards until the year 2024. A 120-second block time is employed to promote minimal transaction times. The initial coin supply is 999,481,516 LTHN, with block rewards issued according to the following formula:

```
Reward=(TotalSupply-AlreadyGenerated)*2-19* 10-8
```

After a final block reward of 29 LTHN per minute is reached in 2024, that amount will continue to be indefinitely issued as a subsidy, yielding about 1.5% annual inflation. The subsidy encourages continued network support and utilization. Without a final subsidy block reward, the incentive to continue supporting the network is minimal. The absence of incentive could have devastating consequences for the coin including lack of miners and cost prohibitive transaction fees.

VPN technical details: non-commercial

The Lethean coin wallet will function as a decentralized marketplace with inbuilt features for peer-to-peer virtual private network connections in two supported modes: the full VPN service and the Browser Extension Proxy service. In short, a Lethean wallet user will act as a client node while a complementary server side exit node provides VPN or proxy services. Interested users of the network can decide to become an exit node, allowing their internet connection to act as a proxy/VPN for other Lethean users in exchange for Lethean coins. It should be emphasized that decisions to participate in the Lethean network as a VPN exit-node or client node are strictly voluntary. Users can transact Lethean coins for any independent purpose outside of VPN and proxy services by using the Lethean wallet.

Users offering their connection to be used by others are termed exit nodes, due to the fact that traffic from networked client nodes will exit through their end network. Exit node users will announce their services via Lethean Service Discovery Platform (SDP) [Figure 1], specifying fee rates in Lethean Coin that client nodes must pay in order to utilize the exit node connection. The SDP also contains all other details needed for client users to make a purchasing decision.

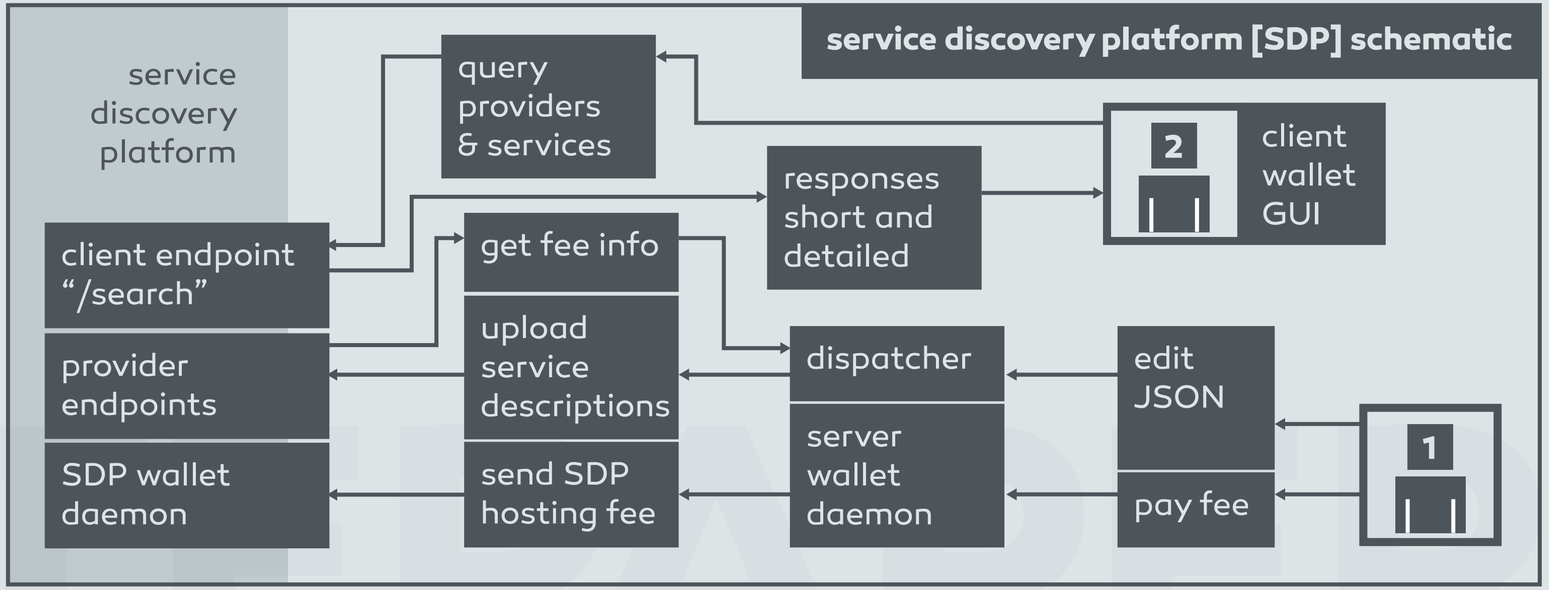


Figure 1, Lethean Service Discovery Platform (SDP) Schematic

Parties interested in acting as exit nodes will broadcast information about the country-level location of the exit node, the IP address of the exit node, speed of the node, the cost of the node in LTHN per minute, bandwidth limitations (if any), and uptime. Nodes will have options to configure number of clients, port and bandwidth limitations. This information is created in a local configuration file on the exit node and uploaded to the SDP. All management of configuration and orchestration of proxy and VPN services on the exit node is done via the 'dispatcher'. We use the term dispatcher to refer to the master facilitator process of exit node permissions and configuration.

Vice versa, users interested in utilizing the peer-to-peer proxy/VPN as clients will select exit nodes meeting their criteria in terms of price/rate in LTHN, location and speed. In contrast with established major VPN providers, our software is configured to keep no identifiable logs of client node activities while providing plausible deniability to exit node operators.

Parties interested in establishing connections to network exit nodes, or client users, will create a service agreement and initiate a connection to the selected exit node. An implementation of the OpenVPN protocol with per-user X.509 certificates will be used to secure connections between exit nodes and client users. OpenVPN is well-recognized as a secure and reliable mechanism of VPN connection due to its use of Secure Sockets Layer (SSL), strong encryption and the signing of messages with HMAC digests [5].

Furthermore, OpenVPN is a portable solution, readily supporting Windows, Mac and Linux; the same three operating systems currently targeted by the Lethean coin wallet and daemon.

After a connection between exit and client node is successfully established, client nodes will initiate a VPN transaction by sending a payment for the initial period of service. For every minute going forward that the VPN tunnel remains alive between the exit node and client user, the client node will remit a per-minute payment. If the connection or expected payment fails between the client and server, the service agreement is terminated; the client node will no longer send LTHN, and the exit node will sever the connection.

Payments are generally made many minutes in advance to prevent service delays related to transaction confirmation time. As the backbone for payments is the Lethean blockchain, the block time of two minutes is significant. In other words, it takes on average at least two minutes for a payment to reach the receiver. To prevent proxy/VPN service interruption due to transaction confirmation times, the Lethean wallet sends payment in advance for many minutes at once. The amount of time is configurable by exit node providers.

Features to host an exit node and/or connect to an exit node will be present in both the graphical user interface and console versions of the Lethean wallet and daemon, respectively. Currently, only a command line interface (CLI) of the dispatcher is available for exit node providers.

Concerns exist related to legal and technical capabilities of exit nodes that nefarious client nodes could exploit. These include but are not related to accessing forbidden material, such as pornography, or copyright infringement via torrenting and other file sharing services. In effect, the Lethean exit nodes will feature options to restrict outbound traffic over specific ports, such as the default torrent client ports of 6881-6889. There may also be specific domains or IP addresses that exit nodes wish to disallow access to for legal or security reasons. Thus, exit nodes have configuration options to disallow outbound traffic based upon IP or domain. Restriction of exit node connectivity will also feature limitation by service type, for example only allowing HTTP, HTTPS or FTP requests.

VPN technical details: commercial

A clear need exists for commercial, professional VPN providers to possess a mechanism to compete in a standardized marketplace. Therefore, the Lethean network will allow commercial VPN providers to advertise their service offerings side-by-side with P2P VPN exit nodes. Commercial VPN providers will list the same items as P2P nodes; location, speed, cost, and bandwidth or service limitations. As with P2P VPN connections, Lethean coins will still be used to transact between client nodes and commercial VPN providers, and payments will still occur on a per-minute basis.

To foster adoption by commercial VPNs and minimize barriers to implementation, we will offer commercial VPN providers easy integration with the Lethean network. The dispatcher has been designed with commercial providers in mind. It is capable of orchestrating connections across machines, and capable of organizing multiple services and endpoints in a single configuration file. As most commercial VPN providers rely on or accommodate OpenVPN connections to their network, the choice of our project to utilize OpenVPN will promote seamless integration with minimal technical challenges.

Challenges

A number of challenges exist in proposing a decentralized peer-to-peer VPN. One of the most pressing concerns is the security of end user data. While VPN data transmission is encrypted from client node to exit node, network requests must then proceed from the exit node to the target endpoint. For example, if a client node makes a non-secure HTTP request, the data flow is as follows: encrypted at the client node and sent to the exit node, plain text to the HTTP server from the exit node, plain text from the HTTP server to the exit node, and finally being sent back to the client node from the exit node in encrypted form (see figure 2).

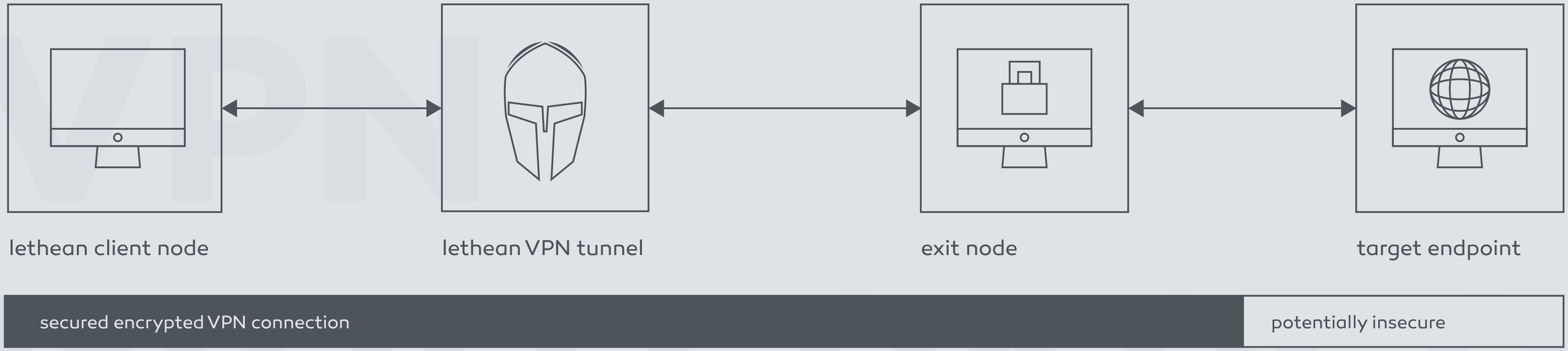


Figure 2, VPN connections and potential insecurities

Counterparties operating exit nodes will have access to non-secure data being transmitted from client nodes. Even secured SSH and HTTPS connections could be subject to potential man-in-the-middle (MITM) attacks on the exit node if client node software does not employ proper certificate authority (CA) validation. In the same regard, exit nodes could tamper with non-secured data transmission, for example by injecting advertisements into HTTP requests. These are the challenges posed by creating a trustless, decentralized system.

To maintain a decentralized VPN and address security, two features targeting consensus-based validation will be included in the Lethean VPN. While no decentralized solution exists to reliably secure HTTP transmissions, HTTPS transmission security can be assured by certificate authority (CA) validation.

Operating systems and browsers generally have in-built lists of known CAs, and this is sufficient in most cases to prevent self-signed and malicious CAs from conducting attacks. One mechanism to improve this is network consultation for CA validity. Exit nodes will submit a request to the network to verify that the issuer of a certificate for a domain matches the proper issuer and expiration according to consensus. Requests failing to meet quorum will be rejected to protect client node data. To address the lack of security offered by HTTP requests, client and exit nodes will have options to disallow HTTP traffic.

To further protect client node security and privacy, DNS requests must be addressed. First, it is imperative that VPN connections force DNS resolution by the exit node rather than the client. This can be ensured through proper OpenVPN client configuration and, in some cases, operating system-level configuration. Second, exit nodes should only use encrypted DNS. DNSSEC is the ideal technology to prevent man-in-the-middle adjustment of DNS records, but few hosts actually implement the technology. Therefore, we will implement system level utilization of DNS over HTTPS (DoH) for exit nodes. A highly reliable DoH server has been made available for public use recently [7], and we feel strongly that utilization of this technology is critical. This assures that outbound data from exit nodes is proceeding to its true designated endpoint irrespective of faulty or incorrect local DNS settings. Further, it prevents exit node traffic from being monitored as easily, ultimately providing more security for the end user.

As the SDP is served from a single centralized endpoint, it would be trivial to block access to the SDP to prevent utilization of the Lethean network. To address this countermeasure, the Lethean daemon will disseminate signed data from the SDP across the network in the same fashion peer lists are disseminated now. Exit nodes will still require direct access to the SDP in order to upload signed data, but client nodes can receive time stamped and signed data from anywhere, as long as the data is validated to originate from the SDP. Client nodes will validate SDP message signatures using hardcoded ed25519 public keys. This ensures access to the entire Lethean network is driven by a decentralized P2P approach and cannot be easily restricted.

Operating a VPN exit node carries inherent risks. Beyond the simple fact of accepting connections from potentially rogue remote computers, a major risk exists in data transmission. Many countries and localities place restriction on internet freedoms, limiting access or restricting access to certain kinds of material such as weapons, pornography, etc. Users choosing to operate exit nodes will be required to understand their local laws, as any sort of traffic could potentially flow through the exit node. The Lethean software will include explicit warnings for VPN exit node operators about these risks.

The transaction scheme for Lethean VPN, where client nodes pay exit nodes per minute of use, poses an issue considering the non-refundable nature of blockchain transactions. It is possible that an exit node could collect payment for few minutes of service but fail to fulfill the duty, either intentionally or unintentionally. On a small scale, the loss of LTHN would be only a few minutes worth for a client node. On the other hand, if an exit node was habitually prematurely terminating connections before fulfilling the expected minute of VPN service, a significant sum of LTHN could be wrongfully received. Our solution is to use a feedback system to mark quality of exit nodes. Client users provide feedback for an exit node after every service period. A composite feedback score is then calculated and broadcast to the client users from the SDP. Our roadmap also includes the capability for exit nodes to offer refunds.

Use cases

There are several potential use cases for VPNs:

Geographically restricted content
Content providers such as YouTube, Netflix, Hulu and many others restrict content to specific geographic locations due to advertising or licensing constraints. A strategically located VPN could circumvent such restrictions.

Corporate and/or government firewalls
The Internet is heavily restricted in certain settings. The Great Firewall of China blocks most popular Western social media and news outlets. Due to the encrypted nature of VPN traffic, it is possible to circumnavigate such restrictions. Furthermore, while most anti-VPN technologies filter or blacklist certain ranges of IP addresses known to belong to popular VPN hosts, such an approach would be ineffective with Lethean hosted VPNs as the decentralized network follows no specific IP address pattern.

Data restrictions and limitations
As 'Net Neutrality' approaches extinction, it is more important than ever to secure and anonymize usage habits. Internet service providers have been compiling data on users' activities and habits, and will charge more money for access to certain activities or resources [6]. Encryption of incoming and outgoing data via VPNs negates their abilities to analyze and restrict access.

Encryption of data
Whether to protect network traffic data from a malicious hacker or 'Big Brother', VPNs are one solution to anonymizing internet usage. Without encryption, any non-secure (non-HTTPS) traffic is transmitted in plaintext, easily readable by a third-party.

Roadmap to succeess

Backed by a solid foundational plan to satisfy a clearly signaled need in the blockchain and security markets, Lethean will be successful due to high priorities of access, portability and marketing.

In terms of access and portability, the vast majority of computer users will be able to access and utilize the Lethean VPN, as the software is cross-platform with current releases for Windows, Linux and Mac. The roadmap also includes plans to release on mobile devices in 2019.

Blockchain based technologies notoriously seldom pay attention to strategic marketing. Although marketing was quiet during the design of the Lethean Proxy/VPN alpha from the beginning of 2018 until Q3 2018, marketing is now being prioritized as the team presents a functional and polished product suite. A major marketing step taken in 2018 was the rebranding from Intense Coin to a proper brand and identity, Lethean.

A professional branding firm with experience in digital global brands was recruited to design the new brand. The Lethean brand aligns closely with our goals of promoting private, accessible and secure internet, whereas Intense Coin was a meaningless moniker and did not accurately represent the full suite of products we have created and continue to develop. An international trademark for Lethean has been filed and is currently pending. Going forward, Lethean will emphasize rigorous marketing to promote awareness and adoption of our products. Currently, the Lethean team includes an expert digital marketer and social media specialist to accomplish these goals.

A detailed product roadmap can be found at our website **lethean.io** [link - click to open].

Changelog

Revision 4 (1 September 2018): Many updates to bring whitepaper up-to-speed with the current infrastructure and components of the Proxy/VPN network and software. Rebranding of ‘Intense Coin’ to ‘Lethean’.

Revision 3 (10 December 2017): Two distinct modes of operation of exit nodes is established (P2P VPN and commercial VPN). Roadmap updated.

Revision 2 (4 November 2017): Revision of Challenges section to remove the need for a centralized server via network consensus driven DNS resolution and CA verification. Add configuration setting for limitation of number of clients for VPN exit nodes.

Revision 1 (31 October 2017): Initial draft.

References

[1] Allied Market Research. SSL VPN market [Internet]. 2017 Aug [cited 2017 Oct 31].
Available from: https://www.alliedmarketresearch.com/SSL-VPN-market

[2] P&S Market Research. Mobile VPN market size, industry analysis and forecast to 2022. 2017 Jan [cited 2017 Oct 31].
Available from: https://www.psmarketresearch.com/market-analysis/mobile-virtual-private-network-products-market

[3] Saberhagen NV. CryptoNote v 2.0. 2013 Oct 17 [cited 2017 Oct 31].
Available from: https://cryptonote.org/whitepaper.pdf

[4] Bohannon J. Why criminals can't hide behind Bitcoin. 2016 Mar 9 [cited 2017 Oct 31].
Available from: http://www.sciencemag.org/news/2016/03/why-criminals-cant-hide-behind-bitcoin

[5] Crist EF, Keijser JJ. Mastering OpenVPN. Birmingham, UK: Packt Publishing; 2015. 367 p.

[6] Save the Internet. Net neutrality: What you need to know now. [cited 2017 Oct 31].
Available from: https://www.savetheinternet.com/net-neutrality-what-you-need-know-now

[7] Cloudflare. DNS over HTTPS [cited 2018 Sep 1].
Available from: https://developers.cloudflare.com/1.1.1.1/dns-over-https/

LETHEAN

THANK YOU