
Intense
Coin

Table Of Contents

Intense Coin
Version 1.3

Intense Coin Team

October 31, 2017

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.

Intense Coin (ITNS) is a cryptocurrency that seeks to address the growing and persistent need for secure internet usage by establishing a peer-to-peer, decentralized, blockchain driven, anonymous virtual private network (VPN). Intense 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 Intense network will offer two mechanisms for VPN connectivity. True to classic cryptocurrency ideals and values, the Intense network will allow end users to host VPN servers and act as exit nodes for peer-to-peer (P2P) VPN tunneled connections. In effect, a decentralized and trustless VPN is created. The Intense 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 encrypted 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 intensely favorable. 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. Intense 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. Intense Coin, unlike conventional Bitcoin-based cryptocurrencies, is based on the CryptoNote algorithm which utilizes ring signatures to mix transactions among multiple receivers for 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. Intense Coin will address 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. Intense Coin will allow these providers to list the prices and details of their service offerings in one convenient marketplace, side-by-side with Intense P2P VPN exit nodes. In simple terms, Intense Coin wallets and products will be to VPN services as *eBay* or *Amazon* are to general goods: multiple sellers from multiple regions will list their VPN capabilities, allowing end-users the ability to freely select the exit node which makes the most sense to them from a cost, bandwidth, speed and location perspective.

Significant attention has been devoted in the conceptualization and development of the Intense network and VPN to avoid affiliation with nefarious end users. As VPNs offer anonymity, it is conceivable that some individuals seek to use such services to avoid association with or conviction for criminal activities. In effect, the Intense P2P VPN has been designed with specific features to restrict access to certain types of network activity such as torrenting. All of these features exist to promote Intense VPN and the Intense 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.

INTENSE COIN DETAILS

Intense Coin exists foremost as a cryptocurrency, based upon CryptoNote and Bytecoin foundations 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, Intense Coins are created by mining blocks of the blockchain, using CryptoNight as the proof-of-work algorithm. However, unlike classic Bitcoin-derived cryptocurrencies, Intense 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 Intense Coins emphasizes the egalitarian philosophy of the product.

The Intense 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 Intense team created a 10% premine to be shared among core members and a 5% premine to be used for bounty rewards.

Intense 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 ITNS, with block rewards issued according to the following formula:

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

After a final block reward of 29 ITNS 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, and the absence of incentive could have devastating consequences for the coin including lack of miners and astronomical fees.

VPN TECHNICAL DETAILS: NON-COMMERCIAL

Intense Coin will function as a decentralized marketplace with inbuilt features for peer-to-peer virtual private network connections. In short, the Intense wallet and daemon will be used to act as a client node or server/exit node for VPN services. Interested users of the Intense network can opt to allow their connection to act as a VPN for other Intense users in exchange for Intense coins. It should be emphasized that decisions to participate in the Intense network as a VPN exit-node or client node are strictly voluntary.

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 specify rates in Intense Coin that client nodes must pay in order to utilize the exit node connection. Vice versa, users interested in utilizing the peer-to-peer VPN as clients will select network users meeting their criteria in terms of price/rate in ITNS, location and speed. In contrast with established major VPN providers, exit nodes will keep no logs of client node activities.

The Intense wallet already provides a mechanism for peer-to-peer communication by means of blockchain transactions and mining. Users' decisions to purchase or advertise VPN services will use the existing network backbone for advertisement and execution of service agreements. 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 according to ping, the cost of the node in ITNS per minute, bandwidth limitations (if any), and uptime. Exit nodes will have options to configure number of clients, port and bandwidth limitations.

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 Intense 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 minute 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 ITNS, and the exit node will sever the connection. Connections will also be severed if the client node exceeds the bandwidth limitation imposed by the exit node.

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 Intense wallet and daemon, respectively.

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 Intense 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 will also have configuration options to disallow 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 Intense 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, Intense Coin 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 VPN providers the option to allow the Intense client to facilitate connections to their network rather than requiring providers to operate an Intense Coin exit node VPN on every server that they maintain. There are extreme security considerations that will prevent most commercial VPN operations from being interested in operating third-party software on their enormous networks. Therefore, from a networking and connectivity standpoint, all commercial VPN connectivity will be simply facilitated and forwarded to the end company. As most commercial VPN providers also rely on or accommodate OpenVPN connections to their network, this will allow simple integration with minimal technical challenges.

A distinct differentiation between end-user offered VPN connections and commercial VPN connections is that the latter, in most cases, will require identification of users. Generally speaking, commercial VPN providers abide by Know Your Customer (KYC) laws and regulations, and require that network users have established some degree of identity with the provider. The Intense software will recognize providers that require KYC documentation. The VPN marketplace will identify providers that require KYC information, and in the event that a connection to a KYC-mandating commercial entity is requested by a user, the relevant information will be sent to the commercial VPN via an API. The Intense services or network will never collect or store any user data. Data requested by KYC-mandating VPN entities, such as name, email and address, will be stored locally in the Intense Coin wallet on end-users machines that wish to use said services, and only transmitted to KYC mandating entities upon request. For a graphical representation of the KYC flow and the general Intense VPN concept, see figure below.

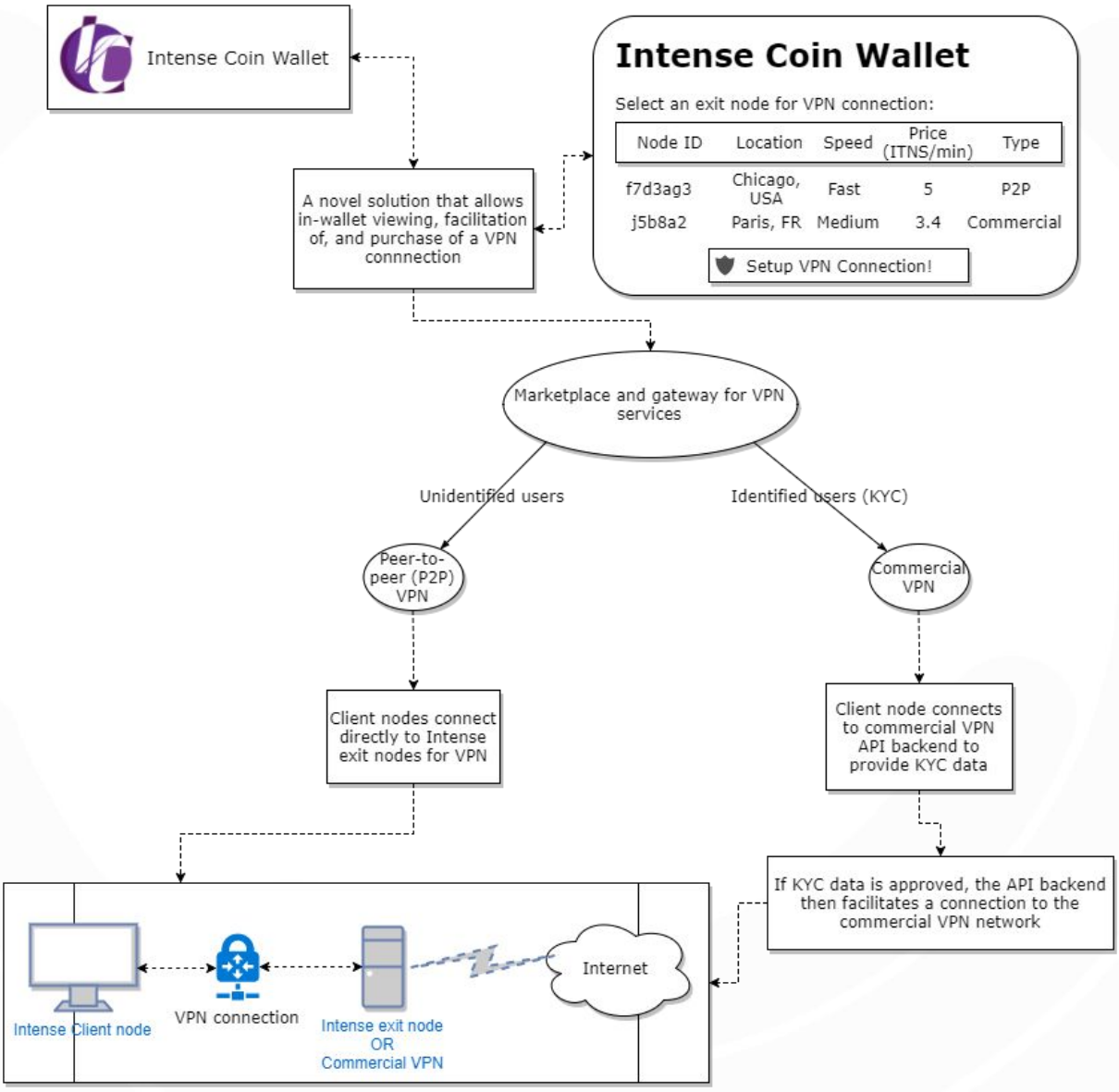

Figure 1, Intense Coin Wallet client and server flow

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 a client node to an 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).

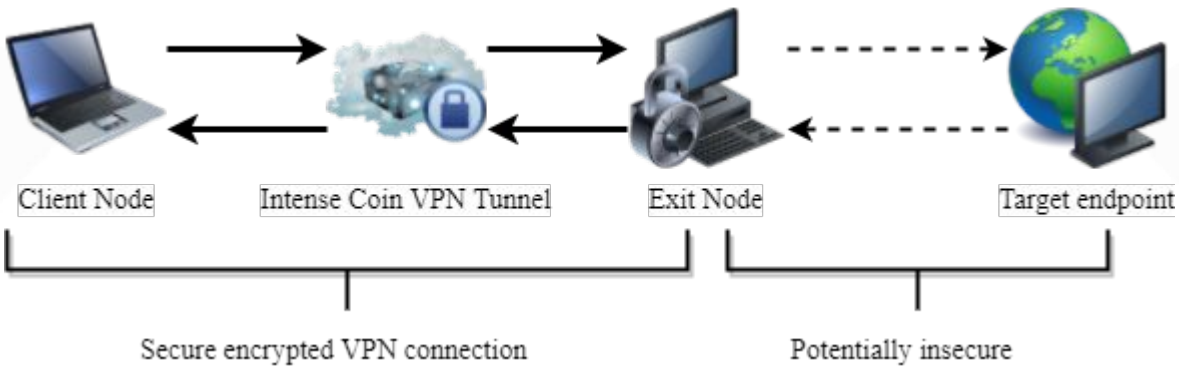

Figure 2, VPN connections and potential insecurities

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. 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 will be included in the Intense VPN. While no decentralized solution exists to reliably secure HTTP transmissions, HTTPS transmission security can be assured by a network consultation for certificate authority 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 requests.

To further protect client node security, DNS requests will be resolved by Intense blockchain peers rather than directly proceeding from an exit node. DNS resolution will not proceed at the client node level at all; the full tunneled OpenVPN connection will direct all VPN requests to the exit node. Exit nodes will not directly perform DNS queries. Outgoing requests from the exit nodes will consult the Intense network for DNS resolution to an IP, and a quorum will be sought by the querying exit node to determine where client node requests should eventually proceed. Outgoing traffic from the exit node (to the target endpoint) will then proceed on a direct IP basis based upon network consensus determined DNS query. This assures that 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. DNS query results will be cached to minimize the performance penalty of decentralized DNS resolution.

While Onion-style routing could be utilized to further increase the security and anonymity of client node transmissions, there are significant downsides to this disseminated form of data exchange. The most significant disadvantage is speed and bandwidth limitations.

Increasing numbers of mainstream and popular websites deliver rich media content with little attention paid to bandwidth usage, especially in the context of social media platforms which emphasize photo and video content. Due to the fact that data proceeds through many clients in onion networking, bandwidth intensive operations suffer dramatic latency effects. Thus, onion-style routing would significantly restrict the browsing abilities of the average internet user. Furthermore, onion routing would not allow definitive routing for users seeking to use strategically geographically located exit nodes to access geo-restricted content. While the Intense team is not opposed to adding optional chaining of exit nodes as a late development cycle feature, it is not an initial priority feature for the reasons discussed.

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 Intense software will include explicit warnings for VPN exit node operators about these risks.

The planned transaction scheme for Intense, 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 a minute of service but fail to fulfill the duty, either intentionally or unintentionally. On a small scale, the loss of ITNS would be only a single minute 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 ITNS could be wrongfully received. One solution is to earmark funds in exit node wallets that were tied to service provision. In the event that VPN service was not delivered successfully, ITNS would then be sent back to the receiver. An issue with this approach is that without protocol-level regulation, such a check could be easily sidestepped in open source software. Due to the ring signature nature of Intense, transactions cannot be easily traced from sender to receiver, thus it becomes impossible to monitor and enforce agreements in a network context.

A more pragmatic solution to the issue of wrongful remittance is establishing a rating system whereby client nodes are able to rate exit nodes following completion of VPN service. The rating system would require checks and balances to prevent manipulation and fraudulent activity. A rating system is planned for implementation in the Intense VPN mechanics following the initial proof-of-concept release.

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 Intense 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 SUCCESS

Backed by a solid foundational plan to satisfy a clearly signaled need in the blockchain and security markets, Intense 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 Intense 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 2018.

Blockchain based technologies notoriously seldom pay attention to strategic marketing. Intense has emphasized rigorous marketing since its inception and will continue to do so throughout the lifecycle of the development, implementation, and dissemination of the product. Accordingly, the Intense team includes an expert digital marketer with over a decade of experience and relevant knowledge in developing, promoting and preserving brands and brand identity.

A detailed product roadmap follows.

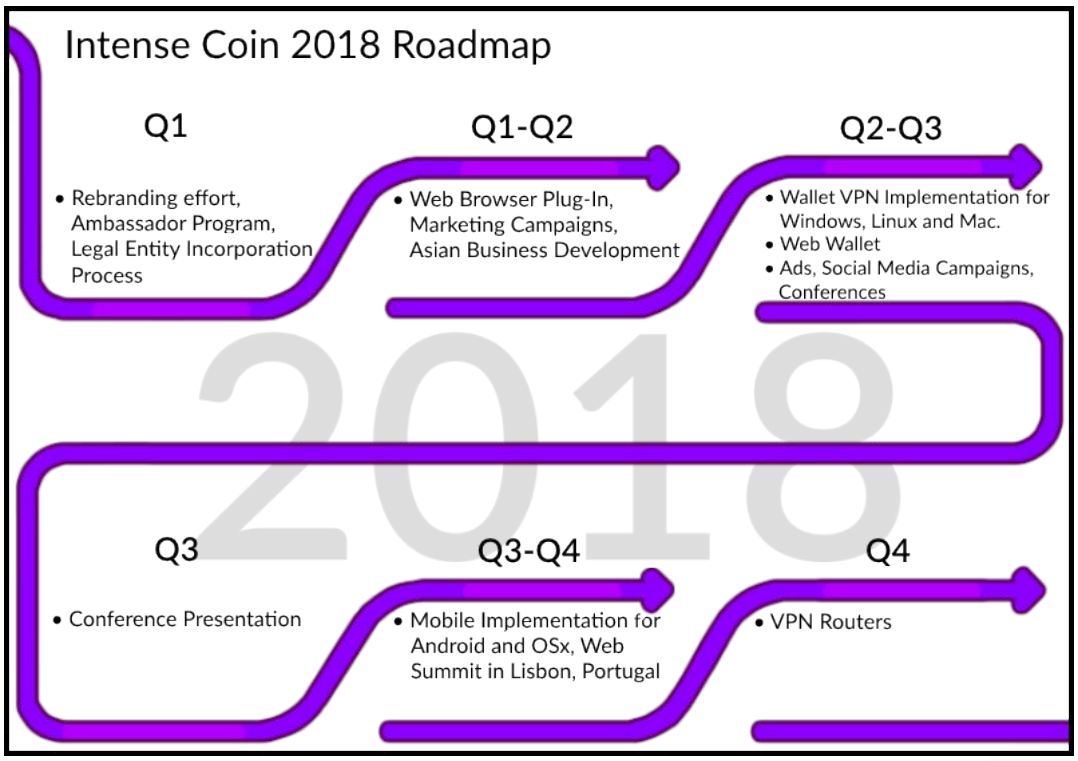

Figure 3, Intense roadmap through 2018

CHANGELOG

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

Revision II (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 I (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