SENTINEL

A Blockchain Framework for Building Decentralized VPN Applications

Sentinel dVPN Protocol Whitepaper

Table of Contents

01.
Intro: Sentinel's Vision

The purpose of the Sentinel ecosystem is to empower universal access to the internet in a trusted and provable manner. This will be done by allowing organizations and individuals around the world to construct cost-effective, scalable, distributed and decentralized networking solutions on Sentinel's Cosmos-based blockchain by taking advantage of:

01	02	03
Decentralized consensus	**Open-source networking integrations**	**Distributed community based node network**

The Internet has created a form of intertwined global consciousness capable of tremendously positive effects. However, the significance and power of the information dissemination capability of the internet is being threatened. There is a rapid increase in global internet censorship and mass data collection and with the ever increasing dependency that people have on the Internet in today's time, this trend of censorship and data collection infringes on the fundamental human rights of access to information and privacy.

The initial focus of the Sentinel ecosystem is to provide a framework for the construction of Decentralized Virtual Private Networks or dVPNs. VPN applications are used by individuals across the globe with the intent of accessing geo-restricted content by connecting to servers located in regions where their desired content is unrestricted, while at the same time ensuring the privacy of their interaction through the establishment of an encrypted connection. Whether the purpose is to access restricted content or to increase the security of their transmission of data over the internet, individuals all over the world are demanding secure, cheap and reliable VPN services.

With the release of the Cosmos IBC, which allows for cross-chain interoperability, Sentinel will be able to perform the role of providing a private networking or dVPN layer within the Web 3.0 infrastructure stack. In the near future it will be possible to build a fully decentralized DeFi application that is:

- Hosted on a Handshake Network TLD
- Has data stored on a IPFS (Filecoin)
- Utilizes computing resources from Akash network
- Integrates with dVPNs built on the Sentinel network to provide both the application and its users with network level privacy and security.

At the time of inception, VPN technology was primarily focused around the establishment of secure tunnels in between the servers of an organization and its members to ensure encrypted data transfer. Over the last decade, the modern consumer has begun to associate VPNs not only with the traditional enterprise focused narrative, but also with an entirely new narrative surrounding their concerns relating to privacy, internet security and global data accessibility. We have seen the growth of the VPN industry blossom as a result of these concerns, growing at a rate of 17.2% annually with the projection of the industry reaching a global market cap of $107 billion by the year 2027.

Current VPN applications available to consumers in the VPN space fail to prove the authenticity of their claims and to keep their promises to the user while assuring users “privacy” and “reliability”, thus creating a major contradiction. This contradiction is being exposed on almost a quarterly basis as of recent years, as leading VPN networks are consistently being exposed for intentionally storing and collecting user data, while at the same time, allowing major security vulnerabilities. The VPN industry is currently operating as a cartel, with a vast majority of the leading brands sharing the same owners. These similar products share the same degree of obscurity, meanwhile consumers lack trust in their back-end functionality.

Contrary to these mainstream “consumer facing” VPN applications, a robust and holistic ‘dVPN’ network (a term initially coined by Sentinel in 2017) has the merits of:

1. **Provable Encryption -** The provability of the establishment of end-to-end encryption between the user and the server which the user intends to access data from, through open-source transparency and application integrity verification systems

2. **Proof of Bandwidth -** Having a system of bandwidth provability which allows for the provision of bandwidth by the server provider in exchange for the agreed upon compensation from the user in a trustless and provable manner

3. **Proof of No Logs -** Ability to provide evidence that no logs pertaining to the user's browsing or data history are being centrally stored by the application developers

4. **Distributed Exit Nodes -** Having a network of ‘exit nodes’ (dVPN servers) whose ownership is distributed amongst many participants who do not know the identity of the user

5. **Distributed Relay Network -** Having a robust relay network with strong governance and participation to mitigate the risk of bad actors, while ensuring that exit-node hosts do not know the identity of the user

The Stakeholders involved in the Sentinel Network include:

Validators - Consensus participants in the upcoming Sentinel - Cosmos Hub who are responsible with securing the network and participating in the governance of the Sentinel ecosystem

User - The end-user who wants to access a dVPN built on the Sentinel framework in order to securely the Internet in a provable manner

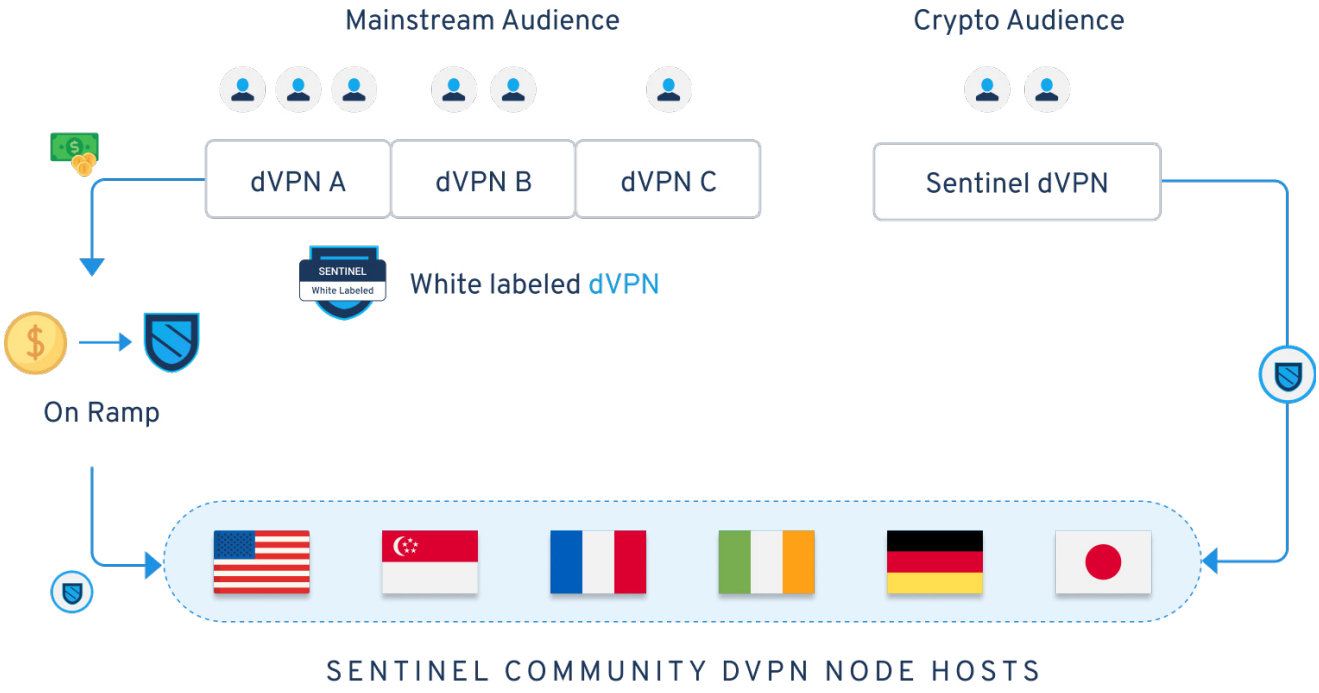
dVPN Node Hosts - Community members intending to monetize on the provision of unused bandwidth to dVPNs built on the Sentinel network, by hosting either an exit node or a relay node (meeting certain required service level thresholds)

dVPN Application Creator - The creator of a dVPN built on the Sentinel framework while using the Sentinel dVPN zone as its infrastructure layer. The application creator is responsible for user acquisition and marketing in order to generate revenue in order to be able to pay dVPN node hosts

02.
Decentralizing the VPN industry

> Sentinel is not a single dVPN application, but a network of independent dVPN applications built on Sentinel's dVPN protocol framework.

It is the goal of the Sentinel ecosystem to decentralize the VPN industry and introduce the 'dVPN' to the mainstream consumer. However, this goal will not be achieved through the launching and maintaining of a single consumer facing application (the Sentinel dVPN), but by first establishing and then developing upon a framework that can be used to create a network of independently operated decentralized VPNs.



dVPNs built on the Sentinel framework may be operated by corporate entities or individuals alike. Sentinel also aims to cooperate with existing centralized VPN providers, helping them to transition their backend architecture to a decentralized structure; allowing these companies to further build trust with their existing client base, while also allowing them to further expand their service offerings.

You may find yourself wondering why an entrepreneur or an existing organization would want to work with Sentinel, constructing a dVPN?

Three key issues that pose as barriers to entry for new and existing VPN companies, alleviated by the Sentinel ecosystem:

1. **Cost and Process of dVPN Application Development -** Networking protocols such as OpenVPN and Wireguard, while fully open-sourced, need to be packaged into a scalable and secure "cross-platform" set of applications. Meanwhile, integrating subscription-based systems and payment gateways provide a tedious example of some of the more basic implementations required when developing a dVPN network. The resource requirements necessary for developing a high-end VPN/dVPN application from scratch is seen as exhaustive by most.

   Sentinel offers open-source, cross-platform dVPN clients that are resilient, secure and highly scalable. This is due to Sentinel utilizing Cosmos-based architecture which offers a public & private key "account management" system in addition to on-chain node querying (more details in future publications). We have ensured that building on top of Sentinel's framework and customizing the architecture is developer-friendly. The overall process will be extremely cost-competitive in comparison to developing one's own in-house VPN/dVPN application.

2. **Management of Nodes and Handling of DMCA requests -** Leading cloud service providers would inevitably restrict server access to exit-node hosts because of the streaming or downloading of pirated content from the node which would undoubtedly attract DMCA requests. Centralized VPN organizations generally have to rely on 'offshore hosting services' which may not provide the same degree of reliability in terms of up-time and real-time customer support that more well-established providers would offer.

   The Sentinel ecosystem removes the responsibility of exit-node management from organizations building applications on the Sentinel framework with the integration of Sentinel's community based node hosts.

   Owners of VPN applications will have the ability to create service contracts and establish certain standards of quality with node hosts in the Sentinel ecosystem, while also not having to manage the ownership of these servers themselves.

3 **Potential Security Threats and the Risks Associated with Hackers -** Closed-source and centralized VPN solutions cannot be peer-reviewed and therefore are not able to be evaluated by unbiased security experts. This can lead to potential vulnerabilities or security risks which have the ability to harm or seriously disrupt the reputation of the company providing the service.

The incidence of a security vulnerability not only puts users at risk by the potential exploitation of their data, but also creates a tremendous lack of credibility in the VPN organization itself which may drastically affect the organization's revenue and sustainability.

This open-source structure provided by Sentinel greatly decreases the chance of a security vulnerability occurring. An example of the strengths of open-source software would be the world's military organizations utilizing Linux as their prefered operating system in a majority of their systems. Linux is fully open-source and is constantly being reviewed by third parties; as opposed to a software suite such as Windows which is closed-source and notoriously known for security problems.

While the Sentinel framework offers the tools as well as the infrastructure to build and operate a robust dVPN service, the owner of the application has the responsibility of acquiring customers and understanding their specific target market in order to deploy effective marketing strategies. It is important to note that product development and execution is only part of the equation. The other part centering around the actual onboarding of users and the establishment of a product that is in demand by the market.

4 key tenets for the success of an effective dVPN application include:

1 **Strong UI/UX -** Applications built upon the Sentinel framework should be indistinguishable from leading VPN services already provided within the industry in terms of the level of user-friendliness and ease of access. Users may not be willing to transition to a more decentralized solution unless the process of their onboarding is seamless, even with an increasing trend in the demand for secure and transparent VPN services. The learning curve for using a dVPN application must be minimized through the use of intelligent design. There must be a strong focus on the particular aesthetics of the application in order to exemplify a strong brand image.

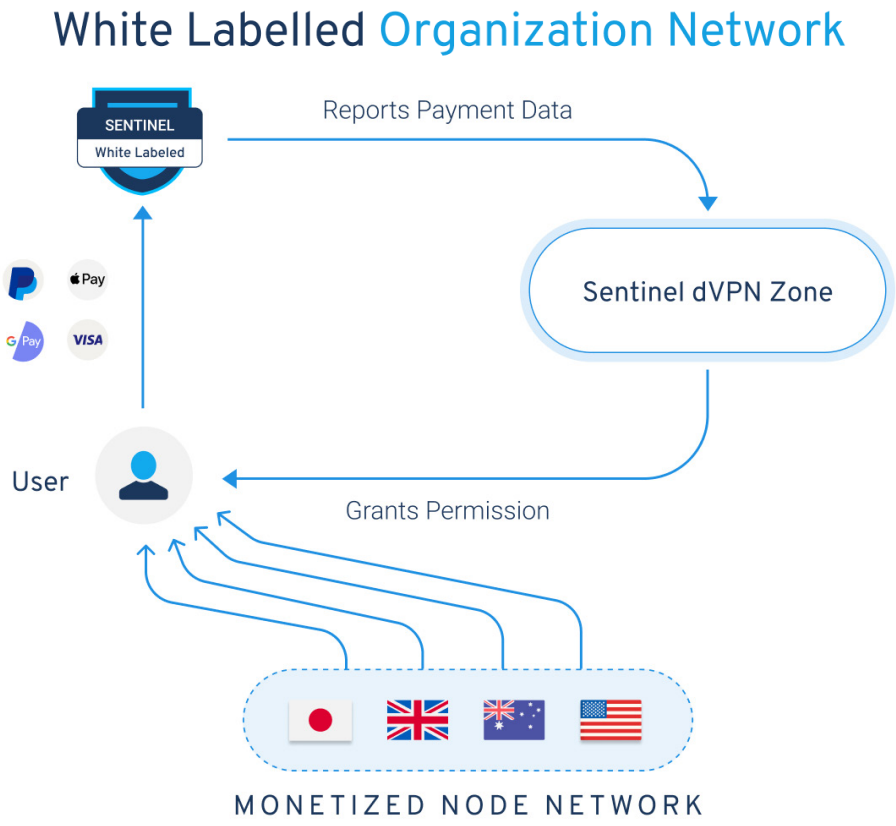
2 **Efficient Pricing Strategy -** The implementation of a pricing model that is not only cost effective but lucrative plays a crucial role when attempting to establish a successful dVPN application. It is important for applications to be able to generate revenue which is then passed down to the node hosts. This enables them to monetize their provision of bandwidth resources; creating a healthy and sustainable decentralized economy. The pricing model employed depends entirely on the target demographic and the type of services offered by the application. In the future, creators of dVPN applications within the Sentinel ecosystem will be able to offer advanced services within their application. These advanced services include the

upcoming relay network along with other enhanced privacy related implementations. Additional services can be priced into users' existing subscriptions or can be monetized based on the exact amount of data consumed. Regardless of the pricing strategy or revenue model employed by a dVPN owner/operator, it is the responsibility of the application's creator to conduct proper due-diligence and analysis in order to arrive at the best pricing model.

3 **Integration of Mainstream Payment Gateways -** It is critical that applications built upon the Sentinel framework offer users the ability to make purchases through fiat-based payment options such as:

Visa/Mastercard | Apple Pay | Google PlayStore | E-Wallets (e.g. Paypal, Skrill etc.)

Having only a cryptocurrency related payment option would create a massive barrier to entry; preventing the average consumer from easily transitioning away from a centralized VPN service provider. While nodes hosted within the Sentinel ecosystem have to be paid through the use of digital blockchain-based assets, dVPN application owners have the ability to monetize their applications through the use of fiat payment channels. The fiat currencies collected can then use an 'on-ramp' service to convert the fiat currency into a digital asset which is then used to pay the node hosts.



4 **Diversity of Routing Protocols -** Different geographies require specific routing protocols to seamlessly access data from the internet while avoiding the interference of potential obstacles. The intricacies and idiosyncrasies of various geographies must be fully understood for the correct deployment of optimal "user-specific" routing protocols in the dVPN application. A networking configuration that performs seamlessly in one geography may be completely redundant in another, thus requiring a customized approach when selecting the appropriate routing protocols for a dVPN application. For example, the OpenVPN protocol is not capable of bypassing the firewalls of several different nations while it functions without any hindrance in other nations.

03.
Overview of Sentinel Cosmos-Based Blockchain Architecture

Cosmos: The Future of Decentralized Cryptocurrency Ecosystems

Interoperability solutions which facilitate the exchange of assets and data between various cryptocurrency powered decentralized networks have the ability to decrease the tribalism in the industry. In this context, 'tribalism' refers to the aggressive tendency decentralized networks exhibit when attempting to establish or show their superiority over their counterparts.

The facts is that certain networks have unique service propositions, enabled by their custom architecture and unique development focus. Interoperability enables participants in the ecosystem to take advantage of the merits of each of these networks simultaneously without having to draw a comparison, allowing for horizontal scalability/specialization.

Cosmos aims to decrease this 'tribalism' in the ecosystem by connecting these competing chains together, effectively decreasing a major divisive influence that would normally keep them apart. The Cosmos IBC module will allow for these on-chain applications to expand their overall target market demographic by catering to a much broader user base, helping to ease the acquisition of new customers by enabling them to accept dynamic cross-chain payments.

Currently, the most significant interoperability initiatives between Cosmos and other highly valuable and respected networks include the interoperable 'bridges' being built from Cosmos to both ZCash, and Polkadot.

The Cosmos ecosystem enables Sentinel to establish and govern its own native chain at the 'Hub' layer. While dVPN applications built on the Sentinel network reside in either shared zones or in their own native zones, depending on the throughput requirements of each individual application.

Chains built using Cosmos have the ability to maintain governance related autonomy, while also ensuring interoperability between other hubs and zones in the Cosmos network.
Unlike with the ERC20 token model, chains built on Cosmos will not have to pay a fee in Cosmos' native token 'ATOM', instead they have the ability to pay in the chain's native token.

Hub and Zone Structure

Sentinel uses the Cosmos Hub/Zone architecture to increase dVPN dApp related scalability by having all application specific transactions and data exchanged on the 'Sentinel dVPN Zone' (or sidechain), while abstracting away the token related transactions and governance onto the 'Sentinel Hub' (or main-chain). Zones will communicate with Sentinel's main-chain (hub) through Cosmos's Inter-Blockchain Communication (IBC) Protocol. A zone can be loosely compared to a type of 'state-channel' that is deployed for efficient scaling.

The 'dVPN' application specific zone will have its own consensus governance which will most likely be a subset of the Hub's consensus validator participants. While there will be no monetary value exchanged at the zone level, incentivization and disincentivization of validators will happen at the Sentinel Hub level.

Using IBC, Sentinel Network's Hub communicates with the Cosmos Hub and other Hubs as part of the Cosmos Network. This not only will enable Services within the Sentinel Network to communicate with each other and accept either the native token SENT or other white-listed tokens, but also to help them connect with other networks within the Cosmos Network.

The Sentinel - Tendermint blockchain can host dApps and or services that operate in their own independent Zones by having specific governance built on top of the Tendermint consensus, allowing their own set of Validators to verify transactions.

Throughput

Tendermint uses a bPOS consensus system wherein blockchains can set a finite number of validators in order to achieve faster consensus, while at the same time protecting the network from 'Byzantine attacks'.

Various P2P communication and privacy solutions will be built on the Sentinel network will rely on high volume, microtransaction-based revenue models. This makes the Tendermint blockchain perfect to support the Sentinel network due to the ability to achieve a high TPS (transactions per second), especially when compared to Ethereum's significantly lower '15 transactions per second'.

Transactions-per-second (TPS) for blockchains using Proof-of-Work (POW) consensus have been relatively

slow and many scaling solutions for such consensus networks require a high capital investment for specialized hardware.

Cosmos uses a unique bonded Proof-of-Stake consensus where votes from a fixed number of validators, with a certain degree of entropy, are accepted by the network at a specified point in time. This increases the overall throughput of transactions on the network due to a finite number of validators processing transactions.

Tendermint's BFT consensus system allows the Sentinel network to achieve transaction speeds faster than that of any currently existing PoW network; PoW networks are encumbered by a lack of definite finality. In bPOS-based systems such as Tendermint, near-instant finality is achieved through the use of a round robin-based voting system utilizing a finite number of Validators by enabling token holders to 'bond' tokens to Validators deemed trustworthy.

Interoperable

The interoperability nature of Cosmos's IBC protocol allows for the creation of a peg (backed by a stable coin) zone. This feature can be developed for chains that are not in the Tendermint or the Cosmos ecosystem.
The utility of these zones will be primarily for cross-chain payments. With this technology it is possible for community hosted nodes operating on the Sentinel dVPN network to accept cryptocurrencies such as Ethereum, BTC, PIVX, DASH, NEO, Dfinity, Cardano etc. in exchange for bandwidth.

Any cryptocurrency can be integrated, regardless if it is built on the Cosmos SDK. This is made possible through the use of 'bridges', which require the establishment of an interoperable connection between the two networks. The Sentinel Hub will be connected to the Cosmos IBC, which will allow for dVPN users to make payments in different currencies or stablecoins that are supported by the Cosmos IBC.

Due to the fact that the IBC protocol can effectively be utilized for communication between different networks that have distinct consensus mechanisms and structural schematics (e.g ZCash/Cosmos), Sentinel believes that the IBC protocol is extremely effective for transaction scalability and dAPP related efficiency through the introduction of the Hub/Zone model.

The technology provided by the Cosmos Network and Tendermint allows us to envision a true free market economy empowered by 'flawless cross-chain payment integrations' that has thus far not been possible with any other platform/network. This is the first step on the long journey of creating blockchain applications that will achieve real world adoption.

Governance

On Sentinel's Cosmos-based mainnet, network governance will be in the hands of the validators. These validators will be democratically determined on the Cosmos-based Sentinel mainnet through the delegation of tokens by holders. The 'Voting Power' or weight of validators is determined not only by historical performance, but also by the amount of tokens delegated to them by Sentinel supporters.

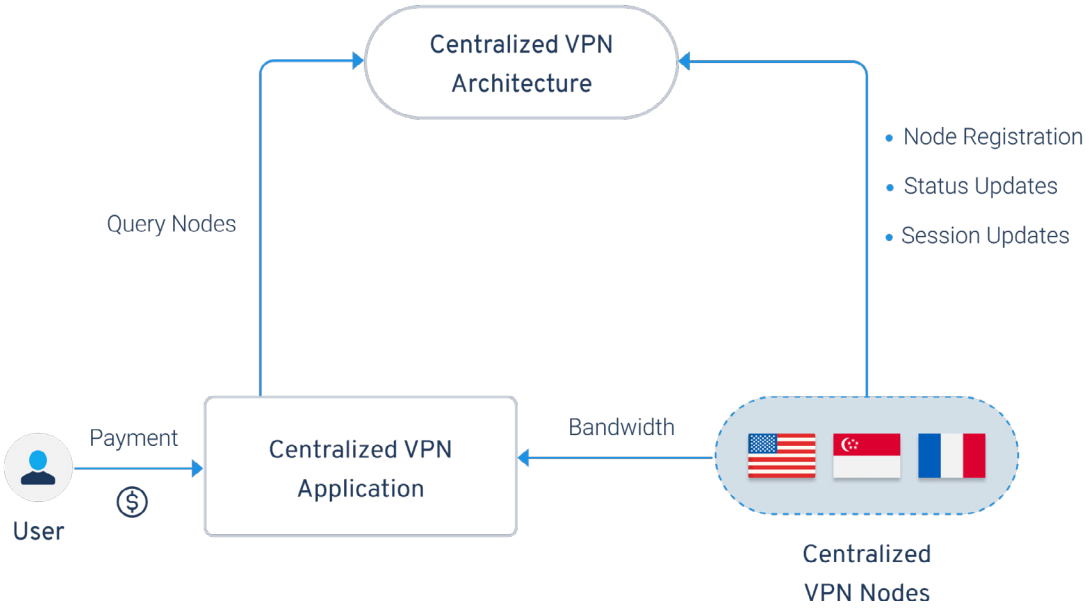
Network Governance Proposals are handled by a set of democratic validators, circumventing the requirement to fork to a 'new chain'. These proposals may include:

- Acceptance of new validators or the rejection of existing malicious validators
- Acceptance of new zones and bridges or the rejection of existing ones
- Changes to supply or the locking of a malicious/hacked account

04.
Overview of Sentinel dVPN Architecture

Centralized VPN architecture is composed of multiple intermediary servers that are required for the governance over a user's permissions as well as for the establishment of the user's connectivity to the VPN node. This centralized architecture requires a high degree of dependency on these intermediary servers, which pose a risk to the networks resiliency due to multiple points of failure as well as multiple points of attack. Down-time of the centralized VPN networks can be attributed to the improper functioning of one or more of these components and can lead to the decrease of user experience and satisfaction

The Sentinel dVPN framework provides an incredible degree of resiliency and security when compared to any consumer-grade VPN. Sentinels architecture minimizes the number of intermediary servers and dependencies. Apart from the account management and creation system that happens completely on-chain, the process of querying available servers happens on-chain. As the blockchain which the application is hosted on will be operational 24/7, with no disruption, as the validator community's infrastructure is globally decentralized (not affected by 1, 2 or 3 data center outages), the up-time and user experience of such an application will far exceed the centralized competitions offerings.



A major contributing factor to Sentinel's architectural resiliency is the decentralized distribution of the computing power that will be required to operate the Sentinel Hub and the Sentinel Zone. The computing power the Sentinel dVPN ecosystem requires to function is not provided by or dependent upon any centralized organization and is instead being provided by expert 'validation' organizations, distributed across the globe and feature highly redundant systems with significant bandwidth throughput and up-time.

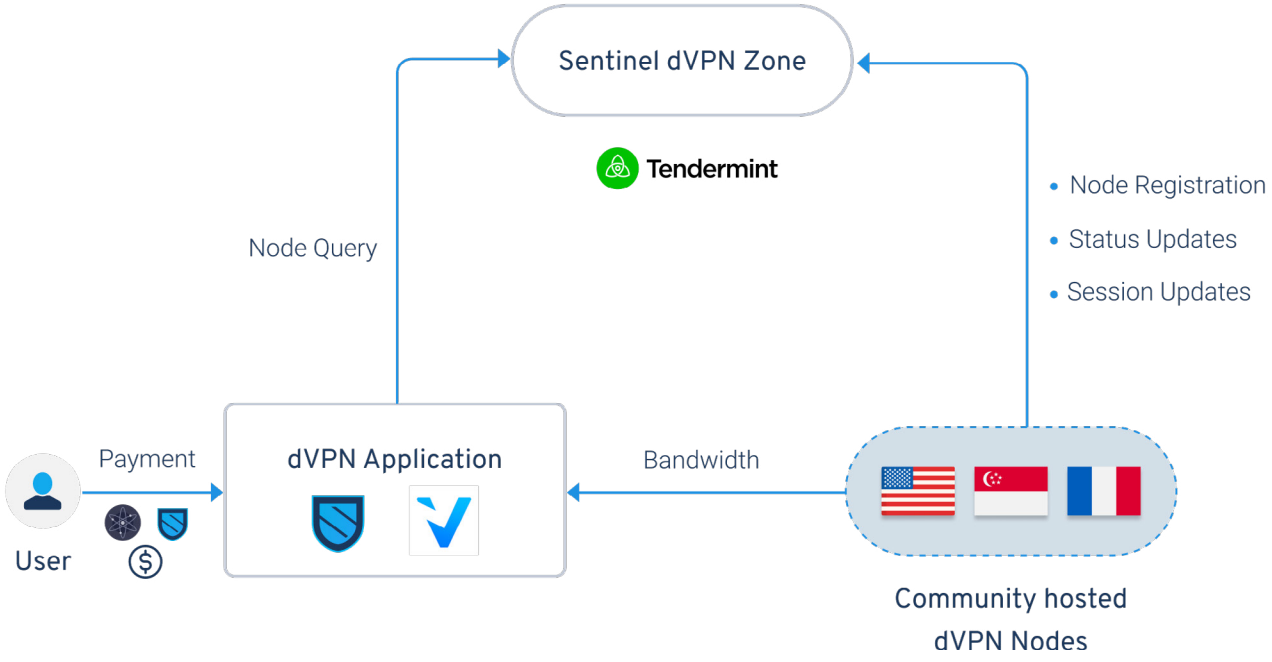
While Sentinel's architecture ensures that a user's anonymity is not compromised by the application itself, the use of Sentinel's upcoming relay network is necessary to ensure that a user is fully anonymized from an exit node standpoint. The Sentinel relay network will allow for users to tunnel their connection through a series of 'relay nodes' which ensure that the user does not directly interact with the exit node.

Sentinel's own proprietary 'proof of bandwidth' protocol ensures trustless and transparent measurement of bandwidth provision from the service provider (community based nodes) to the end-user. The 'bandwidth provability' protocol integrates with the Sentinel blockchain providing a clear track-record for the quality of the bandwidth service being provided and establishes a level of trust between all participants involved. This data is later used to determine whether a node has met the required service-level-agreement in order to avoid penalization.

On-Chain Query

Sentinel's implementation of an 'on-chain' query system is one of Sentinel's most important technical achievements and ensures a highly resilient and decentralized architecture.

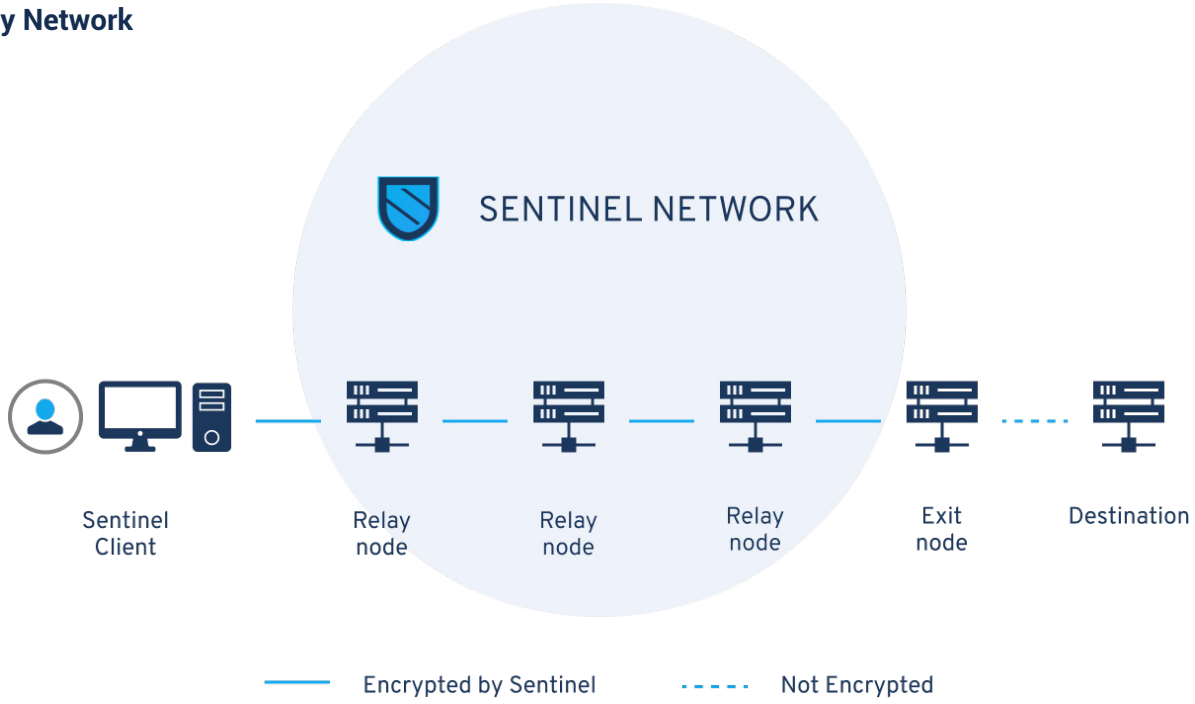
Through Sentinel's dVPN architecture, a connection between the user and the exit-node can be directly established without the requirement of connecting to an intermediate server (e.g masternode for node discovery) that may be controlled by the application developer or a 3rd party. This is done by utilizing the blockchain as a ledger for 'node querying', with nodes having the ability to interface with and store information relating to the node properties and connection instructions. The user's Sentinel-based dVPN application will simply query all available dVPN nodes by reading data from transactions on Sentinel's dedicated dVPN zone, populating a list of available servers. As authentication and identity management already happens on-chain, theoretically the Sentinel dVPN dApp structure's only point of failure (other than networking sybil attack) becomes a potential consensus security failure at the chain level. The only way to compromise the Sentinel dVPN application would be to compromise the validator-driven consensus.



Mainstream VPN applications generally control the exit node, while also controlling and utilizing intermediary query servers that exist between the exit node and the user, rendering the purpose of a relay network redundant as the original user's IP is easily seen.

However, an 'on-chain query' architecture means that the user only has to communicate directly with the chain and not with any other potentially centralized servers that could log their interactions.

Relay Network



A strong relay network is an essential aspect of any end-to-end dVPN solution which fully upholds a user's right to privacy. While neither the creator of a dVPN application built on Sentinel nor any of the participants on the Sentinel blockchain have access to any of the personal information pertaining to users (e.g. IP address), an exit-node hosted within the Sentinel ecosystem would have access to the user's IP address in the absence of a relay network. While a dVPN application has the ability to provide evidence that no logs related to user browsing and metadata are being collected/stored centrally by the application developers, it is currently not possible to prove that logs are not being collected or stored by an exit node host on their local device.

Drawing an analogy to describe a relay network in more simple terms, a connection between a user and the exit-node could be compared to a user making a cellular call to a 3rd party. If the user's intention is for the 3rd party to not be able to see the user's number on caller ID, the user would have to instead use their friend's device as a relay to mask the user's phone number. The user would then have to call the friend who would put the user on hold and call the 3rd party number before merging both phone calls and thereby connecting the user to the 3rd party without exposing the user's data.

Similar to the example of the intermediary cellular caller, a relay network consists of 'relay-nodes'. Relay nodes differ from exit-nodes in operation, as exit-nodes directly communicate with users (in absence of a relay network) while also communicating with web-servers on the internet. Whereas relay nodes only communicate with the user, other relay nodes or the exit node.

A strong relay network is comprised of:

- A large number of participants
- Strong governance
- Multi network integration

The use of a relay system, built on Sentinel, would be primarily for more privacy conscious users who are willing to sacrifice internet speed for improved privacy.

The benefits of a relay network are only realized once a large number of unique participants begin to host relay or exit nodes on the network. If at any time an entity assumes control of a significant proportion of the network, it is possible for the entity to deanonymize the user through a simple but effective 'Man in the Middle' (MITM) Attack. One of the predominant goals of the relay network is to ensure that relay nodes are unable to discern whether they are tunnelling to a user or another relay node. If a user happens to route their traffic through both the attacker's relay nodes as well as exit node, the attacker will be able to correlate the user's IP address and in turn identify that the user is originating the request for the traffic and is not simply another relay participant.

The importance of having a distributed network to prevent a MITM attack in a relay network is shared by the Bitcoin ecosystem, where the intent of mining is to prevent a 51% attack. If a single entity takes control of 51% of the total Bitcoin network mining hashrate, this entity would have the capability to damage the network's

integrity by performing a double spend attack. Bitcoin attempts to combat these monopolization risks in the mining ecosystem with its incentivization mechanism. This incentivization mechanism provides miners with rewards based on their participation in helping to find and verify newly minted blocks on the network. If Bitcoin was a volunteer-based network without an economic design, its security would most likely be compromised. A powerful entity with access to significant hardware infrastructure could easily assume majority control of the mining network. An example of a volunteer driven network is the TOR network. In the TOR network, relay and exit nodes are not incentivized for their participation. Instead they are encouraged to provide their services simply out of shared respect for the ethos behind decentralization. Industry experts worry the TOR network has been compromised by entities who control a significant number of TOR relay and exit nodes. At this point of time, there are roughly 6000 TOR relay nodes on the network with an average of 6 million active users per day. This clearly shows the limitations and or risks of a volunteer-based network.

The success of the Sentinel relay network depends entirely on the number of unique participants. Attracting these participants requires a certain level of incentivization through mechanisms on the network.

Proof of Bandwidth

Distribution of bandwidth in a truly decentralized network shares a common problem with generation of hashes by miners in a Proof of Work network (PoW). This problem revolves around the ability for the service provider (or miner in case of PoW) to misappropriate or falsify the actual amount of work committed. One of the key responsibilities of miners on the Bitcoin blockchain is to confirm the real work (or number of hashes generated) by other miners and ensure that no one is gaming the system to block rewards. Likewise, there is the requirement for a robust architecture in the case of bandwidth distribution on a decentralized P2P network to prevent a bad actor who intends to 'spoof' the amount of bandwidth provided.

An analogy that can be drawn to demonstrate the requirement of a provability solutions for bandwidth distribution networks is the frustrating experience that many mobile phone users claim with their network carrier in regards to their international roaming charges. Most roaming plans offered by network carriers have a restriction on the amount of bandwidth that can be consumed, or at times even bill in terms of the aggregate amount of bandwidth consumed by the user. It is not uncommon to hear accounts from individuals who completely mistrust their carriers after an experience where they believe they have been overcharged and fail to understand how the bandwidth consumption for the roaming bill was calculated.

The provability of distribution of bandwidth is not only important for networking centric use-cases, but also of paramount importance for use-cases centered around storage and computing which also involve tremendous amounts of bandwidth utilization. One of the key goals of the Sentinel ecosystem is to develop and implement the first bandwidth provability protocol, or 'Proof of Bandwidth', to allow for trustless sharing of bandwidth. The

scope of this protocol extends beyond the decentralized VPN applications built on Sentinel, has the ability to be integrated with other distributed p2p resource sharing networks and even mainstream applications.

The first prototype implementation of Sentinel's Proof of Bandwidth protocol happened on the Ethereum chain with the support of an external network of distributed masternodes. These masternodes would observe and measure bandwidth distribution between the service provider and the user, and then inscribe certain properties of the session such as duration and bandwidth consumed onto the Ethereum blockchain. The billing mechanism of the dVPN application would then retrieve this data to generate an invoice that would have to be paid by the user. This prototype architecture functioned as planned, however could not be termed as truly decentralized due to the requirement for an additional masternode network.

The current implementation of the bandwidth provability protocol which is being constructed on Sentinel's Cosmos/Tendermint-based network involves the generation of 'bandwidth signatures' from both the service provider and user. These bandwidth signatures are essentially messages which consist of the bandwidth transmitted in the P2P connection within a pre-configured period of time. The service provider and the user each generate their own signatures which are each signed with their respective private key, and these signatures are then stored on-chain for provenance. In the event of a discrepancy between the bandwidth exchange claims from the user and the service provider (within the pre-configured period of time), the connection will then be terminated due to the presence of at least 1 malicious actor in the exchange.

Bandwidth Signature Variables determined by the dVPN Application Developer:

- The time period for the generation of each bandwidth signature
- Percentage % threshold of discrepancy between the user's and service provider's signatures

Example: The Sentinel 'Proof of Bandwidth' protocol is integrated with 'XYZ' dVPN built on the Sentinel framework. The time period for the generation of signatures is set at 10 minutes and the discrepancy threshold is set at 10%. In the first 10 minutes of dVPN utilization, the service provider inputs a signature on-chain representing 1.05 GB of bandwidth provided and the user inputs a signature representing 1 GB of bandwidth consumed. The discrepancy between both signatures falls between the threshold of 10% allowing for the established connection to continue without interruption.

In the next session, the service provider's signature represents 2 GB provided while the user's signature represents 1.5 GB consumed with the major discrepancy between the two signatures exceeding the threshold, resulting in the connection being terminated.

Payment Models and Escrow:

Monetization of peer-to-peer bandwidth distribution allows for the use of more dynamic payment models than generally seen in the conventional VPN industry. In addition to the general 'pre-paid' system where a user purchases a subscription for a fixed period of time, bandwidth providers (node hosts) have the ability to also set their own pricing per unit (GB) of bandwidth consumed.

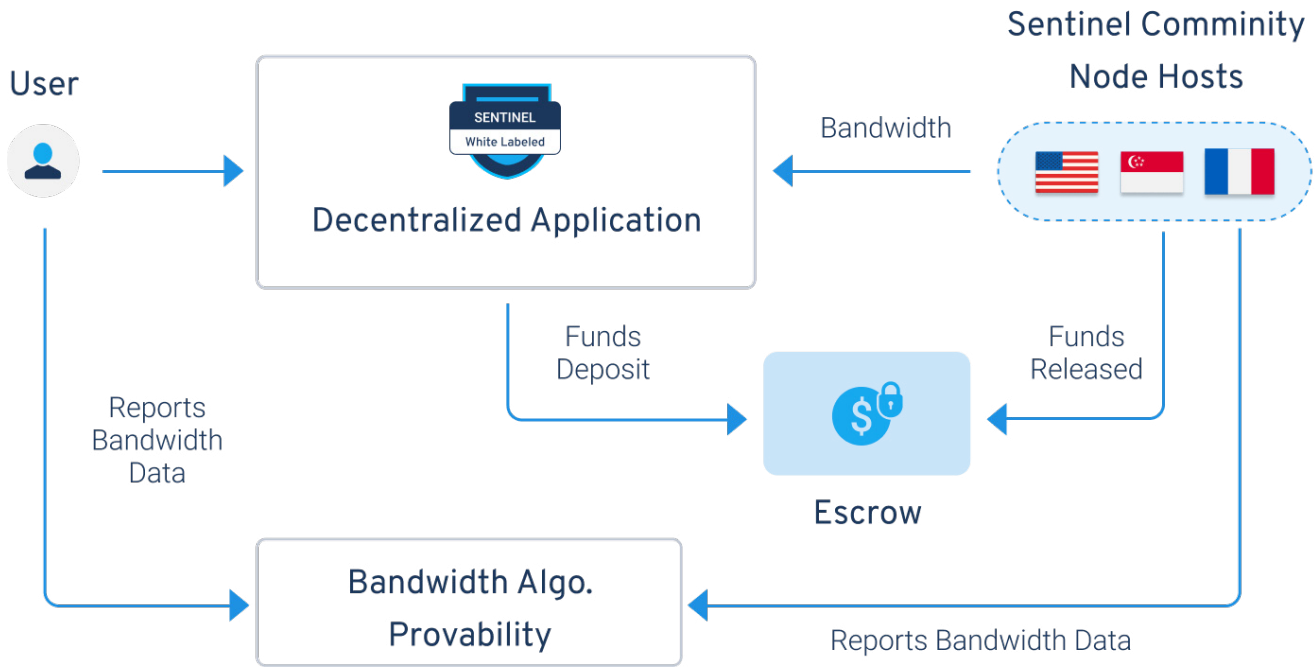
The payment for the use of dVPNs operating on the Sentinel ecosystem will be possible both with conventional fiat-based options (e.g credit card) as well as a large number of cryptocurrencies that will be supported by the Cosmos IBC. However, the pricing of bandwidth through either of the models will be primarily denominated in fiat.

It is important to note that while payment for bandwidth could happen through cryptocurrencies or fiat, the payment the bandwidth provider (node hosts) will make for the infrastructure to host the node will almost always be denominated in fiat. This infrastructure related costs include cloud computing costs as well as electricity costs hardware cost if the node host is utilizing a self-hosted physical setup.

Two key forms of payment models available to dVPN users in the Sentinel ecosystem include:

Real-Time - A real-time payment model is utilized by dVPN node hosts on Sentinel who intend to allow users to pay per 'GB' of bandwidth consumed. In this payment model, node hosts also have the ability to set their own price for their services.
Pre-Paid - A pre-paid model is a more conventional payment model akin to what is commonly seen in the mainstream VPN industry, where users purchase access for a specific period of time. There are no restrictions on bandwidth consumption in a pre-paid model and usage is generally unlimited.

Sentinel dVPN Escrow System - An escrow system is utilized in the real-time payment model between the user and the service provider to ensure that neither of the parties involved can fraudulently impact the transaction. The user is required to lock a certain amount of tokens in escrow before being able to establish a connection, and tokens are deducted from this locked amount on a periodic basis in correlation to the bandwidth being consumed by the user. The accurate measurement of the bandwidth being provided to the user happens through the Sentinel 'Proof of Bandwidth' protocol, which communicates with the escrow to establish a fully decentralized approach to the release of tokens from the escrow.


Decentralized VPN
Sentinel Comminity
Node Hosts
User
SENTINEL
White Labeled
Decentralized Application
Bandwidth
Funds
Deposit
Funds
Released
Reports
Bandwidth
Data
Escrow
Bandwidth Algo.
Provability
Reports Bandwidth Data

05.
Token Utility

The core token utility of the Sentinel token revolves around its functions as a:

- Governance and Staking token
- Medium of Payment for dVPN Subscriptions
- Medium of Payment for Advanced dVPN Services
- Work Token

Governance and Staking Token:

- The Sentinel token is essential for the security of the network, as it is the staking token for Sentinel's Cosmos-based Hub. The Sentinel token will be used to participate in governance related decisions as a form of 'voting power', where the magnitude of a user's voting power is directly correlated with the amount of tokens they hold.
- Users can earn passive income by 'delegating' their Sentinel token to a validator
- Users can host validators and earn commissions from tokens delegated to their validators. This is possible by either appealing for delegation or accumulating enough token to be considered eligible for the active validator set.

The Sentinel hub is built on the Cosmos SDK, and follows the same dPOS-based governance protocol and framework as the Cosmos Hub. The maximum number of validators at genesis will be set at 50. There will be no minimum requirement for self-delegation from the validators on the Sentinel hub.

While there is no minimum 'self-bonding' amount required from validators, validators will only be eligible to enter the active validator set if they have more tokens delegated to their own validator (either from themselves or external holders) than that of the validator with the least amount of total delegation in the active set (the last validator e.g 50^{th} validator). This criteria determining validator eligibility is also enforced by default on Cosmos and other Cosmos-based networks.

Token holders have the ability to earn passive incoming by securing the network through their delegations to reputable validators. Validators have the ability to earn a commission on the staked rewards, with the minimum

validator commission on the Sentinel Hub set at 5% to ensure fair participation and no immediate maximum commission rate.

Stakeholders of the Sentinel token will also have the ability to create governance proposals or vote on proposals issued by other community members. These governance proposals provide the ability for various elements or variables of the chain to be edited without the requirement for a 'hard-fork', or a manual maintenance-based shutdown of the chain.

Medium of Payment for dVPN subscriptions:

- The Sentinel token can be used to pay for a dVPN subscription, however payment for these subscriptions is not limited to the Sentinel token

A subscription for a dVPN service would be similar to the subscription system for a significant majority of popular real-world VPN services. It is quite uncommon to see bandwidth metering-based billing in the conventional VPN industry and VPN services which offer metering generally offer advanced security services and more esoteric routing protocols. A subscription for dVPN services built on the Sentinel dVPN framework will require a pre-payment for the unlimited use of the dVPN through 1 or more devices.

The Sentinel token will be offered as an option for the payment of the subscription. However, users will not be limited to the Sentinel token alone, as the dVPN applications built on the Sentinel framework will have the ability to add real-world fiat-based payment gateways or payment gateways supporting other types of decentralized currencies.

Through interoperability of payments, dVPNs built on Sentinel will be able to reach a wider audience by being able to facilitate transactions from the mainstream market (e.g Google Pay, Apple Pay). If the payment for subscriptions was restricted to the Sentinel token, the customer acquisition process would not be easy to scale and the target market would be very limited.

Medium of Payment for Advanced dVPN Services:

- Advanced services will require users to stake tokens in an escrow system, which would be used for real-time payment and would be governed by Sentinel's bandwidth provability protocol. This structure is indigeneous to the Sentinel Hub ecosystem, thus transactions will be limited to the native token.

More advanced services built on Sentinel will offer users enhanced privacy and a greater degree of trustlessness through the use of escrow services, as well as security focused networking integrations. These services consist

of applications such as relay networks to highly unique and demographic specific networking protocols. Service providers for advanced services (not dVPN applications owners) have the ability to either offer a subscription service or offer the ability for real-time bandwidth billing (pay per GB).

These advanced services will be using the Sentinel 'Bandwidth Provability Protocol' for a decentralized system of governance focused on the metering of the real-time p2p bandwidth exchange. This provability protocol ensures that there is no misrepresentation of bandwidth provision or consumption, without the requirement of a 3rd party masternode system that surveils the connection.

For both subscription as well as real-time billing of these advanced services, users will have to stake their Sentinel token in an escrow system. When using a subscription-based service, payment for the total duration of the subscription is deducted from the locked token amount on an installment basis. For example: a monthly subscription for an advanced service may require 1/30th of the total subscription payment deducted from the staked Sentinel tokens in the escrow per day. For real-time billing, payment will be deducted from the escrow on a periodic basis in direct correlation to the amount of bandwidth consumed by the user, offering a trustless and secure transactional environment.

Work Token:

- The Sentinel Cosmos-based token acts as a work token, thus allowing token holders staking the token to earn rewards. These rewards are generated by the node hosts who provide the bandwidth to dVPN applications built on the Sentinel framework

The strength of the decentralization of Sentinel's blockchain consensus is primarily dependent on the staking participation in the validator governance of the Sentinel hub. Token holders stake their tokens to credible validators to earn staking rewards while increasing the security of the network by effectively increasing the 'cost to attack' for a malicious entity. As the transaction for dVPN services in exchange for digital assets (cryptocurrencies and stablecoins) happens on the Sentinel hub, stakers of the Sentinel token will receive rewards from revenue generated by node hosts on the Sentinel network in exchange for contributing towards the transactional security in the ecosystem.

A percentage of the earnings generated by node hosts will accumulate in a pool before being periodically paid out to token stakers. The value accrual by token stakers from the revenue sharing will be in direct correlation to the aggregate demand for dVPN services from applications built on the Sentinel framework. An increase in the overall number of users and subscription revenue generated from dVPN applications built on Sentinel will result in an increase in the number of required dVPN nodes to service the growing user bandwidth requirements.

06. Hardware Router Integration

The integration of the Sentinel dVPN protocol with Open-WRT based (popular open-source router firmware) networking routers would allow for router owners to become node hosts by easily monetizing their bandwidth. In addition, Sentinel aims to support and integrate with any open-source router which has the capability of being able to apply a dVPN connection over the wi-fi network as a whole. A router-based dVPN would allow for users to avoid installing a VPN application on each one of their devices and the user could potentially create a secondary home network intended only for access through the dVPN.

Ease of Monetization

A benefit for 'bandwidth monetization' focused ecosystems such as Sentinel is the low 'cost-based' barrier to entry for participants as nearly everyone situated in developed economies has a consistent and reliable internet connection. This low 'cost-based' barrier of entry for 'bandwidth monetization' can be compared in contrast to the high 'cost-based' barrier of entry for the mining of Bitcoin, which requires users to buy specific hardware to mine and earn bitcoins.

Sentinel enables anyone around the world to earn passive income by providing their bandwidth resource to dVPN applications built on Sentinel, the hosting of a Sentinel dVPN node on a virtual machine requires some degree of technical experience. This 'technical' barrier to entry decreases the potential of the Sentinel node host community, as it dissuades less tech savvy users from participating. In order to tackle the technical barrier to entry of operating a node, it not only needs to be extremely easy for the average user to be able to use the Sentinel dVPN, but must be as simple as possible to host a node and earn tokens in exchange for providing bandwidth.

Users who are concerned about exposing their residential IP while hosting exit nodes will have the ability to host relay nodes. By hosting relay nodes, owners of Sentinel dVPN enabled routers will be able to stay anonymous from internet service providers while also being able to monetize from users paying for this advanced service.

What is a router and why do they matter?

Routers are devices that are extremely critical to our dependency on the internet, as routers create the gateway to bridge 2 or more networks with each other. In addition, a router empowers a network to facilitate multiple devices, as a router ensures that there is proper load balancing and distribution of bandwidth throughput.

General Features of a Router:

1. Ability to establish a wireless network
2. Ability to apply encryption standards to data routed through wireless network
3. Ability to allow a wireless network to handle multiple devices w/ load balancing
4. Increasing Coverage/Range of Network
5. Dual Band ability to prevent lag

What are the problems with industry-standard routers?

1. Standard are completely closed source and do not offer the public the ability to conduct unbiased code reviews
2. Standard routers do not offer users the ability to tunnel their bandwidth through a provable dVPN network which offers the assurance of security and encryption
3. Standard routers do not offer users the ability to monetize on their excess unused bandwidth

What does this mean?

1. Standard routers can be hacked and manipulated and it may take months or even longer for vulnerabilities to be discovered and fixed, as the codebase is not open to the public (example Linux vs Microsoft)
2. Standard routers do not currently provide users with the ability to securely use a decentralized and distributed VPN application which has the ability to transparently prove the integrity of its back-end operations
3. Standard routers do not enable users to monetize on excess unused bandwidth, thus leading to a waste of paid resources

07. Organizational Structure

The Sentinel organizational structure is primarily composed of the 'Secure Network Technology' Foundation (or SNT) and the for-profit dVPN implementation and development focused organization, Exidio. At this point of writing, both the SNT foundation and Exidio have been fully registered and structured.

While the SNT foundation has a focus of bringing methodological organization and governance to the Sentinel decentralized ecosystem, Exidio is responsible for the technical development of the Sentinel dVPN framework as well as the onboarding of dVPN application creators.

The 'Secure Network Technology' Foundation

1. **Providing Financial and Non-Financial Support to Sentinel Ecosystem Projects -** Responsibility of providing non-financial and financial support to projects and organizations that exist within the Sentinel ecosystem which have the goal of building on Sentinel and adding value to the Sentinel ecosystem.

2. **Driving Adoption -** Mission of driving adoption of the Sentinel Token through the ideating and support of intelligent use cases and mechanisms of utility.

3. **Ensuring Token Economic Viability -** Mission of ensuring a strong token economic structure within the Sentinel ecosystem. It is necessary to monitor inflation and other network parameters with a focus on ensuring that the value of the token is not significantly diluted in the longer term.

4. **Ensuring Economic Health -** Mission of creating a healthy and fruitful environment for validators/nodes/other service providers in the ecosystem. The design and maintenance of robust economic structures which can ensure that service providers will be able to meet their breakeven costs and also receive a rational premium for their time and efforts.

5. **Addition of Ecosystem Partners -** Facilitating partnerships between the Sentinel ecosystem and entities that would add value to the Sentinel ecosystem and drive use of the protocol as well as adoption of the token.

6 **Global Community Expansion -** Expanding the global Sentinel community through the maintenance and support of the various regional groups and the corresponding management of the regional group ambassadors. The SNT foundation is responsible for ensuring that the structure of the ecosystem is compatible for different regions and that the design of the ecosystem doesn't dissuade any specific geography.

EXIDIO

The Sentinel ecosystem is rapidly evolving from a more obscure and anonymous network to a transparent real-world ecosystem that aims to service the requirements of the mainstream consumer. Exidio is a for-profit implementation focused organization that has the mission of 'Providing Secure Access to the Web 3.0", by contributing to and implementing the Sentinel dVPN and Sentinel's Cosmos-based blockchain infrastructure. Exidio will be working with entrepreneurs as well as existing companies in the VPN space to either construct a new dVPN application, or transition an existing VPN network onto a dVPN network.

While Sentinel focuses on providing an environment that hosts the various components of a holistic dVPN network, Exidio will be focusing on implementing white-labelled dVPN applications and carrying out required customizations.

The VPN industry is projected to become a $107 billion market by 2027, and VPN entrepreneurs globally are taking advantage of the increased consumer demand for VPN services by implementing white-labelled solutions. White-labelled solutions offer the benefit of decreased go-to-market costs and require less tech expertise and resources to manage.

Exidio's focus on contributing to Cosmos primarily revolves around:

1 **Development of Utilities -** Development of meaningful and creative utilities that can be implemented by other developers in the cosmos ecosystem (e.g the Exidio multi-sig/joint accounts deployment)

2 **Development of dApps -** Development of useful and efficient decentralized and distributed blockchain-based applications in the Cosmos ecosystem (such as the Sentinel dVPN) that have the ability to provide real utility to even the mainstream user

3 **Contributing to the Cosmos SDK and Tendermint core —** Contributing to the proposed roadmap and also working on optimization and efficiency of the current codebases of Tendermint and the Cosmos SDK.


SENTINEL
www.sentinel.co