DECENTRALIZED DATACENTER

Abstract

Our Internet is centralized. Data, compute and the Internet all flow through datacenters that require huge capital to set up and operate. This has caused one of mankind's most important resources, the Internet, to become powered by a small set of centralized companies.

These central sources of data flow are contradictory to the values of what makes a free and open Internet. Today, as Web3 emerges, it has become apparent that while the mission of many protocols is to decentralize key functions, many of them run primarily through centralized datacenters.

It is impossible to have a decentralized Internet with protocols operating on centrally controlled datacenters. We believe there is a way to create a decentralized Internet on the back of Web3 economics.

This document outlines our proposal for building out the technology and potentially the economics to facilitate the deployment of this type of decentralized Internet infrastructure.

Introduction

The Internet has been perhaps the most important technology in society’s progression in history. There has never been a single, more used, consolidation of knowledge and capabilities. As the World begins to develop more and more technological breakthroughs, development continues to be outpaced by the need to access, store, and compute data at higher speeds with more security.

Web3 is driving the shift to a decentralized, distributed, non-authoritative version of the Internet. New network technologies are being invented without the need for a centralized, authoritative network. Codes, hardware sets, and distribution of technologies are being replaced by core protocols that live in an edge first environment, distributed and authenticated by a consensus of computers instead of a transport to the nearest datacenter. While the development of Web3 resolves an extraordinary amount of issues in privacy and control, it lacks a core infrastructure designed for the same purpose capable of managing the Web3 Internet.

The core values and purpose of Web3 cannot be achieved with the infrastructure we have access to today. These technologies are best powered in a data layer that enables processing large amounts of data closer to end users termed the edge.

Currently datacenters are built vertically in large, centralized settings bringing traffic and data requests to them in layer1. Taking the centralized datacenter model and decentralizing it horizontally, closer to the end users is what edge computing is. Currently edge computing is in its infancy, and Web3 is using the paradigm somewhat with nodes that work together to solve a common equation, i.e., blockchain mining. Our proposed decentralized edge takes this paradigm even closer to the end users and aggregates distributed capacities to provide processing power and file storage in the same, very secure network layer (layer2) as the end user. This solution offers a robust, redundant, distributed datacenter service that is more efficient and effective than the current centralized datacenter of today.

The solution therefore must be an infrastructure that can support and house Web3 technologies and protocols in a distributed and decentralized manner.

To eliminate the need for a central authority the network should have a structure capable of communicating and routing data to any participant in the network that meets the operating principles of the network. This will create a global decentralized and distributed datacenter network that is not only efficient but also robust, highly scalable and capable of global integration and with high security measures.

In order to accomplish this, a decentralized universal data network must be designed that can securely and conveniently house these new Web3 protocols and networks with, at minimum, the same layers available from existing datacenter providers.

Data networks today have three core pillars:

- Security
- Processing
- Storage of data

Centralized datacenters currently focus on these core pillars in vertical stacks of computing devices, storage servers, and firewalls within one building, each handling the task they are designed for working within different layers of a network.

We believe an effective decentralized alternative can natively provide increased value by taking advantage of Web3's design paradigm. Capabilities such as:

- Organic security features
- Redundant file replication
- Zero knowledge level privacy

- Interoperability
- Scalable nodes
- Sharding
- Simple onboarding

Furthermore, this network must encrypt data paths and transport layers, aggregate the entire network of nodes into a single processing environment, be secure on the transport of storage, processing, and recipient layers and have redundant layers of security for end client exposure.

Proposal

We propose the creation of a distributed edge network of nodes capable of transporting, storing and validating data and users. At its simplest, the network must be efficient in its connectivity to the storage systems, secure in its transport layer, private in its readability by any network keeper, and available globally regardless of downtime in certain regions or nodes.

The nodes must be secure, incapable of reading documents, capable of sending and receiving requests and data, and incentivized to maintain the network and act in good faith with the network's purpose. Each node should also be able to connect and communicate with every other node in the network for efficient connectivity.

This network should be redundant against node corruption, bad acting, and downtime. No users should ever have the risk of latency or slow load times with a data request. This can be done through sharding and replicating storage of each shard of data across the network of nodes. The economics and process will be documented in the Node Economics section. Groups of nodes will be assigned responsibility for different data, and secondary groups for redundancy of an entire group of nodes going down or bad acting.

Accessibility

To make a universal infrastructure usable and secure, the network should house two layers. These layers enable a system where the network becomes both accessible and convenient as well as remaining secure in all its capacities.

The first should be the onramp layer for basic network access and initialization. This is where the network will be capable of integrating with systems and cloud processing as

well as managing the ground level traffic. Having this layer allows for the network to be both accessible for easy onboarding and create redundancy for the second layer to be secure from intrusion.

The second layer should house the secondary and robust encryption level and house node authentication and connection layers. This two-layer system allows for the network to manage traffic and create a simple connection to the network while also allowing for a secure and highly protected housing system for the core infrastructure where the node network will communicate and be accessed through.

Security Requirements

The network's security should be built on three standards of security. 1) encryption and technical security 2) incapacity for data exposure 3) repercussions for any bad acting. The node network enables this when combined with crypto economics, BSD security & encryption, and data sharding.

Simplistically the network’s data should be encrypted and secure, have the inability for anyone but the authorized user to access any portion of data, incapacity for anyone to authorize themselves, and economics to incentivize

This is the foundation of a universal infrastructure’s security. There should be privacy-based security to protect data from attack, access, readability or corruption. There should also be a system built into the network that literally prevents any unauthorized entity from accessing data or authorizing themselves to do so. Additionally, any attempt should have repercussions as the enforceability of a rule determines its efficacy.

This begins with the proposed enterprise class firewall system built on top of the OS using both core and expanded features natively available within BSD. The firewall allows fully redundant, encrypted transport layers within our network of nodes. It needs to be a robust defender and referee of networks and have advanced features and systems that allow the inclusion of multi-factor authenticated nodes to work within Layer2. Every node has an instance of the firewall running within the OS and through our clustering technology, all nodes’ firewalls find each other and work in unison.

Global aggregation is allowed through the utilization of VxLANs and encapsulated VLANs to create a grouping of Layer2 subnets that interact with each other, shielding them from Layer1 traffic as a typical firewall would. These interactive subnets allow each node to join within a particular subnet based upon several logic mechanisms (Rtt,

Rttd, latency overhead, among others) and the subnet has designated certain properties within the clustering system for packet delivery and resource delivery within the cluster. This is increasingly important to allow the addition of process aggregation and storage of files onto the Layer2 network as the firewall is providing the encryption sets for the data paths, as well as using its analytics to determine best placement of processes and storage packets for mission critical hosting.

Privacy

A universal infrastructure is the goal for connecting the entirety of current and future projects on a system that neither breaks a user's privacy nor has the capacity to break a user's privacy.

In current systems the development of privacy comes down to two scenarios.
1. Central system that promises not to break privacy and is held judicially accountable.
2. A system such as a blockchain that is incapable of being rewritten, broken, or read.

While privacy usually goes hand in hand with security, the housing of privacy in a decentralized and distributed network infrastructure has three key components it must contain.

1. Encryption
Blockchains SHA-256 encryption level protects against reverse engineering data and making it readable. This is the first layer of any data's privacy protection, making it impossible to read against current computational power or brute force attacks.

A network must take all requests, data, identities, and keys and encrypt them at the highest standard available at the client level, leaving no room for exposure.

2. Sharding
The division of encrypted data on a network creates both capacity for efficient redundancy, lighting transportation, and increased security of data across the network.

Sharding works by taking a piece of data, dividing it into a defined number of pieces, tagging each piece according to the parameters set out in the network's code so it can be called as a whole, and distributing the pieces of that data to different nodes across a network. This prevents any single point from having access to the entire file at any point. Even if the encryption is broken an intruder only can gain access to a fragment. We believe in order for this to align with web3 principles the sharding should not rely on a central metamap point but instead adds the metadata to the shard itself. This is

an important distinction empowering data to sit live within a decentralized environment while adding to its ability to remain encrypted.

With the threat of quantum computing and phishing, encryption alone is not sufficient. A secure network must also be redundant and unalterable. This is minimized by deploying rotating encryptions at all levels of the network, utilizing a rotating encryption set on each end point, as well as an encryption on each shard of each file. This is a laborious, processor heavy function, but by utilizing aggregated processing capabilities, this is accomplished very efficiently with massive compute cycle overheads.

3. Economics
To prevent any node from becoming malicious and exposing, copying, or failing to respond to data requests, economics are put into place to discourage bad acting and incite good acting on the network.

Performance

This edge-first and interconnected network of nodes can create a uniquely efficient and robust performance system capable of handling high traffic. The combination of the edge network, interconnected node communication pathways, and sharding of data into small files will allow for data to be transported, stored, and called with extremely high efficiency. Additionally each node increases the network's compute capacity in its entirety.

Using an embedded firewall within the OS of each node allows the creation of a processing layer for users entirely in layer2. Layer2 allows function within a more secure and higher performing network layer, and a decentralized layer2 allows for more efficient consensus rewards as well.

Current solutions employ the distribution of whole files, which both take long periods of time and clog transport channels until the transport is complete. Because only portions of files need to be sent when data is in shards, and they can be stored anywhere, the network becomes extremely efficient. The transport of 100 shards reduces the transport time exponentially due to the size of the data being transported in comparison to a whole file which would be 100x the size. As such, transport may only take milliseconds per shard and each shard is being transported from different locations at a near simultaneous rate, making the compilation of a data chunk that much more efficient.

Due to the shards of data, files can be replicated throughout the network. Each shard takes up fractions of space and can be transported efficiently as explained previously. As such, in combination with economics, a file will never be vulnerable to being incomplete or unavailable. Should a portion of nodes go down, the next available node containing the data shard will become responsible for the data request and/or storage.

An important piece to this proposed solution is the ability to utilize different encryption capabilities and rotations which would require great amounts of computing power to create and decrypt when necessary. By architecting the system to cluster available capacities, we could dramatically increase the performance of sharding and transporting files. A unilateral layer2 decreases dependency on layer1 pipes, while placing the processing, security, and serving of data within the same network layer as the end user. The same way moving files locally on two switch connected computers is faster than moving the data across the Internet, this type of aggregated edge does the same thing with processes, file storage, and data services globally.

Reliability

A decentralized computing network is always available and always accurate in its internal referencing (ledgers, records, etc.), even if many of the nodes are not participating in the network for whatever reason. Our proposed aggregated solution allows users to continue processing and aggregating data at all times, especially as the network continues to grow.

A proprietary network protocol would be put in place allowing simultaneous multi-casting of data packets across the network of nodes. That would allow users to perform in a totally lossless capacity within the network. Nodes transmit and receive all data across all available network mediums installed on the board of the node. Nodes have ethernet, fiber, wi-fi, LTE, TVWS, and usb-a and c available for network operability on the node itself. All processed packets are transmitted across all network hardware options on the node and the first packet delivered wins.

This allows users to operate networks in all manners and opportunities.

Having this capability and dependability of a lossless network, allows users to reliably remain connected to every node, and nodes to the network, at all times. It also creates new opportunities for users beyond storage as the global decentralized network grows.

This network could provide CDN, global data transport, clustered decentralized application hosting and massive data processing capabilities to be used for research,

or large mathematical needs.

Processing and Hosting of Protocols and Serving of Data

Node clustering allows the network to host systems, protocols, and other data services. All of the nodes within this network are already aggregated at the processing and storage level of the network. When requests come in for data service, most requests are coming already within Layer2.

Through the VxLAN capacities explained within the firewall portion, all nodes within the network would aggregate their processing overhead into the computing ocean and work in real time with each other fully as a cluster. This is a very efficient, and powerful way to process data services.

BSD could be chosen to build the network OS on top of due to its universally available driver sets and hold within the current market technologies. This would allow us to architect the platform to eliminate the need for central computing environments by taking the core and moving it to the edge fully and applying the aggregation technologies to compute as a single decentralized engine. The true edge implementation essentially serves as a virtual datacenter in a box. It includes everything to manage, orchestrate, integrate, pool, track and monitor platforms sitting in the edge. A simultaneous multicast network protocol would allow us to decentralize and distribute clustering through multiple communications means like CBRS, TVWS, 802.x, 5G and more giving it low latency and zero packet loss. Traditional datacenters rely on hardwired fiber and copper networks, and still have packet loss amongst the switched network because they only have one medium for delivery.

Currently Web3 protocols are processed via a transactional paradigm system, with specific equations and processes for writing to the public blockchains. This focus is power intensive and segments each process into a specific set of nodes working on a specific set of functions in unison. Our proposed paradigm would create the processing ocean, storage capacities, and security the network needs and provide that to host protocols atop. This decentralized, distributed datacenter would enable new and emerging markets of users needing connectivity due to the core features natively available within our architecture. By expanding the global edge network, we could provide many hosting features needed by new communications companies to reduce their dependence on Layer1. As our network expands, protocols could reach new users within our organic Layer2 through partnership with companies and networks destressing their Layer1 backbones.

Private sub-networks can be created and can remain independent or clustered on demand to service the complex needs of specific workloads. In the event that a node is compromised, it is removed from the cluster and the other nodes in the network would continue performing their operational tasks without any network downtime.

Node Economics

Nodes will be divided into classifications and groups. A random selection of nodes will be classified for the data request and responsible for the file request. A secondary group will exist as replication of the file should an entire class be corrupted or influenced to bad acting. Each group will be responsible for a portion of the data. When a user requests the data and a transport request of the entire file is called, each group will be informed simultaneously. Each class will then be responsible for the transport of the file. The first node in each group to respond to the request will be rewarded for their participation. Additionally, upon the data request all nodes through proof of replication will be given a smaller reward for their maintenance of the network.

Current Datacenter Paradigm

In a typical firewall, Layer1 is translated to Layer2 for whatever is plugged into it. Most traffic is backhauled on Layer1 to a colocation or further upstream to process the data request. This puts the burden of protection on the customers on the ISPs Layer2 (think home routers, business firewalls, etc.). In an intrusion, the entire network is exposed at Layer1.

Current firewall solutions depend upon the passing of packets organized and layered throughout the World in several steps:

1. Datacenters to store and distribute data upon requests which must be protected from intrusions on Layer1.
2. ISPs to distribute Internet service and protocols to end users which must be protected from intrusions on Layer1 and defense needs are passed downstream to their end users.
3. End users of ISPs that live in layer2 of the ISP itself.
4. End user devices.

These network layers require a full pass, non-pass type of network flow.

Storage System Design

Harnessing the power of new clustering technologies allows one device to house the firewall, file storage, and data processing controlled by a single operating system. The OS allows for each vertical technology to live in a decentralized state, aggregating available overheads of each node, and bringing them into one processing center within the network. This means that every node has its own firewall, its own storage capacity, and its own available memory to seek out and aggregate with other nodes within the network processing all data requests entirely in layer2. This creates an aggregated, decentralized network allows for massive processing capabilities to enhance the security of everything else in the network.

All files stored within the decentralized node network are sharded through a process that breaks the files into fragments, and due to the decentralized, yet aggregated processing capacities, the ability is created to write an encryption to the shards with an embedded, software based meta mapping. These files are then passed throughout the network of nodes and stored in a cross-replication pattern, ensuring that all of the shards for one file are stored hundreds of times throughout the nodes, but no node holds one hundred percent of the shards to a single file.

An encrypted VxLAN is used specifically for the transport of shards between all of the nodes. This VxLAN creates the layer2 and allows for traversing of subnets, relying entirely on an algorithmic based tagging and BIP32/64 key match to retrieve and restore files at a defined mount point by the end user and owner of the data. Decentralization of the network and processing centers protects the data at all times from loss. By storing the files in this decentralized manner, the network is not exposed to variables such as network downtime by a group of nodes, intrusions as key pairs for each node will not match after the rotation, and a global layer2 based network helps to eliminate layer1 security challenges that exist in today's network.

All the nodes within the Network are already aggregated at the processing and storage level of the network edge. When requests come in for data service, most requests are coming from Layer2 as the user has already been encapsulated within the edge at an entry point through partnership with other Web3 and communications companies to deliver that user. Layer1 data requests are traversed and processed in Layer2, fully in the edge before being transported back to Layer1 if that is where the request originated from. All nodes within our Network aggregate their processing overhead into our computing ocean and work in real time with each other fully as a cluster. This is a very efficient, and powerful way to process data services.

This true edge implementation serves as a virtual datacenter in a box, and includes everything to manage, orchestrate, integrate, pool, track and monitor platforms sitting

on top of the network. Web3 benefits from a simultaneous multi-cast network protocol to allow decentralization and distribution clustering through multiple communications means like CBRS, TVWS, 802.x, 5G and more giving it low latency and zero packet loss. Traditional datacenters rely on hardwired fiber and copper networks, and still have packet loss amongst the switched network because they only have one medium for delivery.

These services are clustered together within many Layer2 clusters and aggregated in a multi-cloud aggregator for transport around the world to our other clusters within the network. This creates an agnostic delivery method for packets in a decentralized global manner, eliminating challenges of hosting protocols within Web3. As the network expands, protocols can reach new users within a fully secured Layer2, destressing Layer1 backhauls.

Private sub-networks can be created and can remain independent or clustered on demand to service the complex needs of specific workloads. In the event that a node is compromised, it is removed from the cluster and the other nodes in the network continue performing their operational tasks without any network downtime.

Consensus and Economics

An important part of decentralized networks is the ability to reward and empower participation in providing assets and capacities to the network itself. The network is a multi-level authenticated edge node network. There are requirements for participation from all decentralized nodes, and we have developed a manner of consensus for proving both the capacities available to the network, as well as the successful storage of shards and data on each node.

Our monitoring and control system monitors uptime and available processing, memory, swap, and hard disk space of each node in real time. This allows our storage system to decide which nodes to write the shards to, which nodes to write the replicate shards to, and which nodes will provide computing capacity to create the keys to the encryption of each shard, as well as the store of meta map information within the set. To achieve this, each node must report information back of its capacities to all of the other nodes within the network.

This process also allows for the compression of grouping of shards for transport across VxLANs during large demand periods of reconstruction of data or rebuilding of file data in the event of node loss.

In providing proof of capacity each node simply has to provide proof of the ability to compute overhead capabilities of the number of logic algorithm cycles that can be

performed based upon the percentage of processing power the particular node is providing to the aggregated network cluster (*o)*:
C=P/Q*(√t*o)+[sR-sT] C=Capacity
P=Number of Processors in Node Q=Number of Cores per Processor
t=Time reported to process rTTD{rTTr} (ms) o=Overhead logical equation
sR=Disk space reported sT=Disk space taken

Other variables begin to be added into the overall proof of capacity such as network transmission statistics as well.

Economically, we can produce the first reward to each solving for C in an 86400 second variable for reporting capacity daily:

RW1=SP*PMA | C / (# of nodes in network*C) * RW1

The second reward is generated after each node provides proof of storage of the assigned file. This can only be completed after proof of capacity, which is reverified upon each shard creation within the logic. Proof of successful storage is universally applied as:

Pr[out = accept : (Φ, S) ← hV, Pi(prm) , (out, ∅) ← hV(Φ), P(S)i(prm)] = 1 In our combined approach, we will require a simple recheck against $C\Delta^{\circ}$ = {if} Pr[out = accept : (Φ, S) ← hV, Pi(prm) , (out, ∅) ← hV(Φ), P(S)i(prm)] = 1 1 must be returned at all times and be larger than *C*
To calculate the reward, we simply assign RW2 variable as a determined percentage of SP

RW2=SP*PMB+[*C* / (# of nodes in network**C)*]