Project Proposal of RadiumBlock High Performance Endpoint Q2 2023

1.0 Summary

Proponent	RadiumBlock (RealWeb, LLC) an LLC registered in the United States with EIN 87-2225143
Date	July 1, 2023
Requested Allocation	914.5 KSM ($22,050 USD, based on EMA 7 value of $ 24.112)
Recipient Address	EwR2jzx7gZSjxCXbkVZRm39W2fWGJtwXYYftQYdVfcJjtt4

Short Description:

The RadiumBlock team, an infrastructure provider for the Polkadot/Substrate community, is seeking reimbursement for the provision of RPC services for the Kusama networks for Q2 2023.

2.0 TLDR;

- RadiumBlock is a high performance infrastructure provider for the Polkadot/Substrate ecosystem.
- We operate one of the highest performance RPC service in polkadot ecosystem https://www.comparenodes.com/global-node-comparison/407c5245-0c6f-4abe-be49-1ff0b25a2938/
- RadiumBlock requests reimbursement for
    - Kusama RPC endpoint
    - AssetHub/Statemine RPC endpoint
- RadiumBlock's RPC include:
    - Archive node based RPC endpoints
    - Support both websocket and http for RPC requests
    - 12 location PoP
    - Use our on-prem high availability hardware at collocated data centers
    - Better cost and decentralization
    - Low latency access across the world

3.0 Budget Q2 2023

As stated in our previous proposal, RadiumBlock has moved to a fixed price model for the RPC services.

Usage For Q2 2023

- Our Kusama RPC nodes have served an average of 38 million responses per day
- Our Statemine/AssetHub RPC nodes have served an average of 1.5 million responses per day

Network	Monthly	Quarterly
Kusama Relay Chain	$5500	$16500
Statemine/AssetHub	$1500	$4500
Sub Total	**$7000**	**$21000**
KSM to Fiat Conversion Cost - 5% (Fees charged by exchanges)		**$1050**
		$22050

4.0 About RadiumBlock

RadiumBlock is wholly owned by RealWeb LLC. RealWeb has been in business since 2004. Every year, our team manages millions of dollars in AWS infrastructure, making us one of the industry's most dependable and trustworthy web hosting companies. In addition, our engineers have extensive experience managing data centres and business infrastructure. We harness our expertise and experience in building reliable infrastructure services for the future of web3.

RadiumBlock is an active and known participant in the Polkadot/Kusama community. We participate in the Polkadot and Kusama Thousand Validator Program, offering validator service to several other chains.

We are active infrastructure providers in the DotSama ecosystem. Some of the services we provide are

- High Performance RPC endpoints including high demand endpoints such as Kusama, Polkadot, Astar, Statemine, Statemint
- White Label validators (Node-as-a-Service)
- DevNet as a service (fully managed DevNet or TestNet)
- Snapshot Service snapshot services (validator and active snapshots)

5.0 Infrastructure Highlights

We offer a scalable, enterprise-grade infrastructure that can auto-scale to handle traffic bursts and provide services in different regions around the world, while still delivering low latency responses. Additionally, the infrastructure is designed to be resilient and fault-tolerant irrespective of any downtimes in our service regions. The failover mechanism will patch over traffic from a failed data centre to other healthy data centres with minimal disruption. To ensure a stable and optimal infrastructure, our team works around the clock using several monitoring tools.

The prominent features of our Endpoint services are:

- Low Latency through Custom Endpoint Delivery Network
- Monitoring and Observability
    - Endpoint availability and latency in different parts of the world
    - Endpoint performance and load in each region of the world we deploy
    - User experience of our Endpoint on the polkadot.js application
    - Monitor the blockchain stats of the nodes.
- Auto-scaling and Load Balancing
- Fault Tolerance
- Live Rolling Updates and Upgrades

Our mission is to continuously improve and innovate in order to meet the evolving needs of the Web3 ecosystem. We have significantly evolved our infrastructure resulting in the following:

- Hybrid On-Prem + Cloud computing strategy
- Expanded Edge locations
- Security upgrades

2.1 Hybrid On-Prem + Cloud strategy or Why we mostly left the cloud

A little commentary on why we made the switch from a cloud only approach to a hybrid public cloud + on-prem computing strategy could prove illuminating. Cloud computing has two primary benefits. The first benefit is simplicity - in launching a simple application using fully managed services. Our expertise in cloud from managing infrastructure for enterprises equipped us to build a complex blue green deployment approach on cloud.

The second benefit is scalability - scaling the compute capacity up or down based on load that is highly irregular. Swings in compute demand can be elegantly handled in a cloud environment without degrading the service quality. A beneficial side effect is that it helped us estimate the computing capacity needed when provisioning such a service.

Of these two benefits only the second one ever really applied to us. However the place we are at now, having run the endpoint service for several quarters, we have a fair idea of steady state demand allowing for provisioning of on-prem resources to match the demand.

We also learned about a significant downside to cloud, particularly for blockchains - cost - specifically cost of egress bandwidth. Blockchain by its distributed nature is bandwidth and compute intensive in trying to keep the chain in sync.

All of these factors lead us to try to achieve the best of both worlds - by provisioning steady state compute capacity on-prem and bursting to cloud during unusual spikes. Furthermore, when amortized over 3 years, the savings in compute and bandwidth cost allowed us to channel capital back into increasing the reach and quality of our endpoint service.

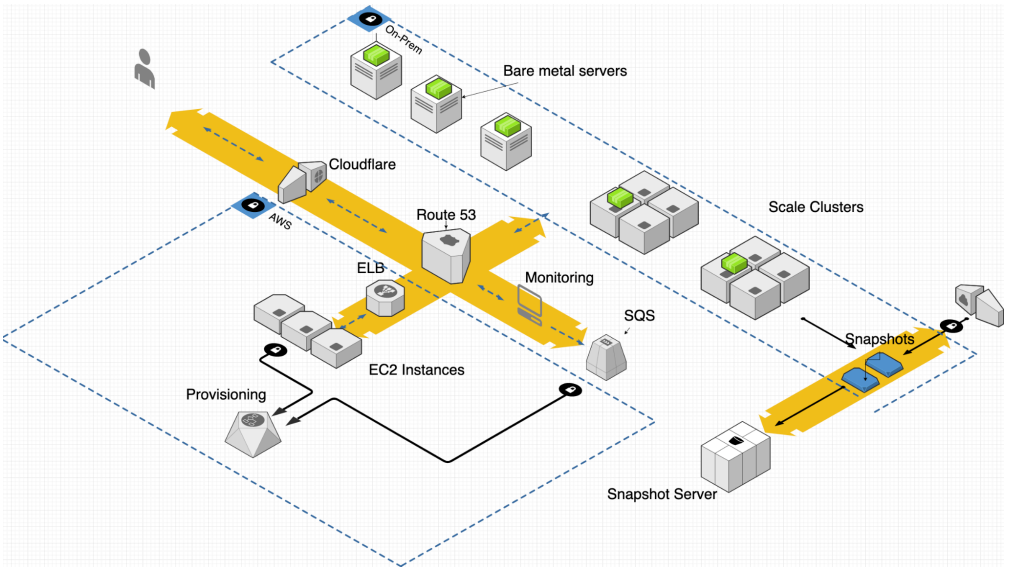
What is our on-prem/private cloud?

Our on-prem aka private cloud infrastructure uses a combination of dedicated servers and a platform called "Scale Computing Platform", something similar to VMware. Presently, we have scale computing clusters deployed on the private racks we rent out from major data centres in 4 locations: Chicago, Sydney, London, and Singapore.The scale clusters we deploy comprise of 3-6 node servers and a standby server for redundancy. The scale clusters are capable of self healing - auto migrating instances within the cluster should one of the servers fail. We use enterprise hardware on these nodes with Intel Gold/Silver CPUs or similar, NVMe SSDs and high speed networking. In the other locations we operate, we have full or partial colocation rack space.

The Architecture

The figure illustrates a high level architecture of our endpoint service. Our shift to a hybrid computing approach required a rearchitecting of the load balancing strategy. We have switched to DNS based load balancing to route traffic to one of our on-prem endpoints running on our Scale Clusters or bare metal servers. The DNS based routing is both load and geography aware - routing the user request to the nearest available endpoint node. By design, bulk of the traffic is handled by the scale clusters and bare metal servers with a smaller portion of the traffic, capacity spikes and redundancy handled by our AWS based compute deployment.

In addition to edge server proximity, several latency saving optimizations like OCSP stapling, TCP stack tuning are applied to our servers.



2.2 Expanded Edge locations

The savings in compute and bandwidth cost allowed us to channel capital back into increasing the reach i.e. more endpoint locations. We are at 12 locations worldwide including South America, Africa and India. The full list is as follows:

Santiago, Johannesburg, Chicago, Silicon Valley, Frankfurt, Madrid, London, Hong Kong, Mumbai, Singapore, Tokyo, Sydney. We at RadiumBlock believe an endpoint delivery network leveraging distributed edge locations is the best way to dramatically decrease latency and make blockchain technology more accessible.

2.3 Security upgrades

We have made a concerted effort to buttress our security practices.

- Access to the servers are permitted only through a Bastion Server where every keystroke is logged, and scrutinised as part of monthly audit. The Bastion based ssh management service uses 2 factor authentication and enables timed access revocation, role based access control.
- Session keys and controller keys are stored in a hashi vault with access limited to two of our most senior admins who have been with us for over 10 years and us the two directors.
- We ensure our colo partners have SOC2 certification.

These steps are in addition to classic security practices we have learned from 2 decades of LInux security management.

The following lists the Risk Mitigation measures in place :

- Our DDoS protection is two-tiered with our servers hosted on both Cloudflare and AWS
- DDoS protection is enabled and disabled based on probable threat perception