GM All, I’m Kai from Baryon.

1. Entity name and location

Baryon, Seoul in Republic of Korea

2. Infrastructure location

Regions across the world.

3. What kind of hardware do you run? Baremetal, cloud-based…? In what geographic regions?

- Multi-Cloud & Multi-Region

In addition, we are currently utilizing 5+ major cloud services such as AWS, Azure, GCP, DO. By keeping ourselves cloud-agnostic, we could provide consistent node operation service to the networks we participate.

4. Technical make-up of team (elaborate on no. of dev ops engineers, experience, etc.)

We have experienced dev ops engineers who have deep skills in Docker, K8S, Ansible and Linux. We even encourage our dev ops engineers to fully have CKA, CKAD and CKS certificates to better meet the required needs.

5. Years of experience

We have 5+ years of node operation experience with multiple networks including Cosmos, Flow, Solana and Mina. And, our node operators have always been at the top of the testnet competition that we participated so far.

Baryon members are all experienced engineers/contributors for many protocols. Our engineering team has plenty of experience in running nodes on major protocols listed below. We want to note out that we never have experienced single slashing event by any chance during numerous years of experience.

6. What other networks are you running validators for?

Archway, Umee, Persistence, Omniflix, Sui, Tgrade, Rizon and so on.

mintscan.io

Interchain Explorer by Cosmostation

Interchain block explorer and data analytics for sovereign blockchain networks.

7. Based on your participation in any previous testnets, mainnets, are there any best practices to be aware of? What are some things that made previous testnets, mainnet launches successful and/or things to avoid that have gone poorly?

Things to DO

1. Community Engagement: Foster an active and engaged community around the blockchain project. Encourage community members to participate in testnets, provide feedback, report bugs, and propose improvements. A strong community can help identify and address issues more effectively.

2. Documentation and Guides: Provide clear and comprehensive documentation and user guides for validators, developers, and end-users. These resources should cover topics such as setting up validator nodes, interacting with the blockchain, and developing decentralized applications (dApps).

3. Network Upgrades and Governance: Establish a clear governance mechanism to facilitate decision-making and network upgrades. This allows the community to collectively decide on protocol changes, parameter adjustments, and improvements to the blockchain.

Things NOT to do

1. Rushed Launches: Avoid launching a mainnet or even a testnet prematurely without sufficient testing and community engagement. Rushing can lead to critical vulnerabilities and instability, undermining user trust and confidence.

2. Ignoring Feedback: Actively listen to feedback from the community and promptly address reported issues. Ignoring or dismissing user concerns can lead to dissatisfaction and diminish the credibility of the network.

3. Centralization Risks: Strive for a decentralized network by encouraging widespread participation from validators and avoiding centralization of power or control. Decentralization enhances the security and resilience of the blockchain.

8. Are you planning to play any additional roles in the dYdX ecosystem (e.g. market maker, trader, indexer, front-end, other)?

Yes. We are trying to build some front-end testing tools by using dYdX API so that those who are not famillar with dYdX can onboard the platform with ease.

9. Any notable contributions in other ecosystems that you would like to highlight for the community?

Baryon members are all experienced engineers/contributors for many protocols. Our engineering team has plenty of experience in running nodes on major protocols listed below. We want to note out that we never have experienced single slashing event by any chance during numerous years of experience.

As a professional node operator, our job is to secure networks all the time, which means that node operators have to be ready 24/7, 365 to deal with unexpected network and cloud platform issues. Our security team always respond promptly and professionally when we encounter node issues since we have multiple security alert systems.

- Node Agent: monitors the status of various machines.
- Independent Agent: monitors the validator status from outside through RPC.
- Prometheus & Grafana
- Security

Security is one of the areas where validators should put significant considerations. Although we cannot disclose specific architecture here due to info sec issue, we will give you a brief walkthrough on how we approach this area:

- As an active user of HSM/KMS, we developed our own in-house KMS that securely handles every operation that involves the use of the private key. Since our KMS maintain secure audit logs to keep track of the keys for security purposes, abnormal and/or unreliable activities are detected immediately.(For certain networks that have network latency due to their blockchain nature, we may not use this software to maintain high uptime.)
- We have proprietary software for machines, too. To maintain real-time protection, the proprietary software detects any abnormal activities or events (within 100ms) and immediately puts the situation under control. Not to mention, firewalls are in place, ensuring that only the ports that are used by the validator itself are opened.
- Reliability / Performance

We have experiences and know-hows on ensuring high availability, stability and performance. To illustrate further on this, we will lay out how we have operated nodes with aforementioned list of projects:

- Pre-analysis and Architecture Design

Our architecture puts emphasis on the most optimal performance as a node operator. This includes an optimal machine load and reduced network latency. This sometimes results into very different validator architecture approach even among the Cosmos family projects. For instance, the approach we took on building the architecture for Cosmos and Terra was significantly different.

1. Sentry / Validator Node Isolation

We always separate the validator node from network and protect the validator node with multiple Sentry Nodes. Indeed, our validator node only establishes private connections to our multiple sentry nodes so that it could be protected. Moreover, we employ Reserve Node in case of emergency. The current architecture protects Baryon validator node from DDoS attack.

Contact

Homepage: https://www.baryon.guru/

Contact: contact@baryon.guru

Discord: kai_baryon