# An overview of Kiln’s Cosmos-based blockchains infrastructure practices

As we run validators on several Cosmos-based blockchains, significant effort has been devoted to automating their setup and maintenance. This enhances our efficiency, resilience, and also reduces the chances of human mistakes.

In this post, we’ll explore how we’ve built our system and the daily tools utilized to ensure smooth operations. Let’s dive into the specifics of our Cosmos validators infrastructure.

## Kiln validators infrastructure

Our infrastructure is deployed on Kubernetes across various cloud providers, including AWS and GCP, but mainly bare metal solutions like OVH & Data Packet are managed by a central control plane.

We’ve standardized on large servers, which allows us to run multiple nodes for different blockchains on a single machine. This approach gives us great flexibility in where we run our nodes, primarily across Europe and Asia. It also enables dynamic adjustments of the CPU, RAM, and disk resources as needed. However, for blockchains with high block rates, like Injective or dYdX, we use dedicated servers equipped with high-frequency CPUs.

Our entire system is managed through a GitOps workflow, offering several benefits such as a reliable source of trust, a comprehensive history, and the integration of Continuous Integration processes.

We’ve also fully automated the bootstrap and maintenance of Cosmos-based chains, including default configuration setup, snapshot management, and upgrade procedures. This level of automation streamlines our operations and ensures consistency across our deployments.

## Security & resilience

Our security strategy is comprehensive and multifaceted, ensuring the protection of sensitive data and the uninterrupted operation of our infrastructure:

- Key management

: All sensitive information, especially validator keys, is securely stored in Hashicorp Vault. This system not only provides robust security but also facilitates easy access when necessary.

- Constrained access

: Strict policy rules are in place, allowing each node access only to its own key. This limitation is crucial for preventing unauthorized use of keys and preserving the integrity of each node.

- Network isolation

: Nodes within the same blockchain network can communicate with each other but are isolated from the rest of our infrastructure. This network isolation per namespace is a key security measure, preventing potential cross-contamination or breaches.

- Port management

: The only ports open to the public are P2P ports, with dynamic configuration of node IPs, This enhances our operational resilience, allowing us to swiftly relocate nodes if necessary in response to outages.

- Geographic distribution

: The combination of these security measures makes it easy to move validators when needed. This mobility is essential for maintaining uninterrupted service and quick response to any network issues.

- Operators wallets

: For an additional security layer, operator accounts are managed exclusively via hardware wallets like Ledger. This practice ensures that even in the event of a compromised system, the operators' access remains secure and untouchable.

[

950×782 14.6 KB

](https://europe1.discourse-cdn.com/standard21/uploads/dymension/original/1X/853d6da0df208ca77866ef19317454fb891b1b50.png)

These measures uphold a high-security standard across our infrastructure, safeguarding our validators and the reliability of the networks they support.

## Remote signing with Horcrux

Initially, our configuration included running a single validator per chain, supplemented by a spare located in a different geographical location.

As we evolved, we embraced the use ofHorcrux cosigners, which substantially enhanced our system's security and efficiency.

[

792×653 7.85 KB

](https://europe1.discourse-cdn.com/standard21/uploads/dymension/original/1X/783b4e72144f0ba5731432f927ae7ec1f0637ed9.png)

- Sentries

: For each validator key, we now deploy at least two sentries. These sentries are strategically distributed across different geographic zones to ensure diversity and mitigate the risk of simultaneous downtime.

- Cosigners

: Alongside the sentries, we operate 3 Horcrux cosigners, which is essential for maintaining the integrity and reliability of our validation process.

- Colocation for Reduced Latency

: To optimize performance, the cosigners are often colocated within the same servers as the sentries. This proximity minimizes latency, critical for maintaining swift and efficient validation processes.

- Network

: In this architecture, the sentries are the ones interfacing with the public P2P network. In contrast, the Horcrux cosigners are configured to operate exclusively over a private network, reducing the possible attack surface.

- WireGuard Mesh-VPN

: A key element of our setup is the use of a WireGuard mesh-VPN. This VPN creates a secure, private network that envelops our nodes. The Horcrux cluster, in particular, communicates over this VPN, ensuring that our internal communications are shielded from external threats.

This evolved validator architecture underscores our commitment to not only maintaining but continually enhancing the security, efficiency, and resilience of our blockchain operations. By leveraging advanced technologies like Horcrux cosigners and WireGuard VPNs, we ensure that our infrastructure remains robust and capable of adapting to the ever-evolving landscape of blockchain technology.

## Monitoring

To monitor all our validators efficiently, we rely on two sources of metrics:

- CometBFT Metrics:

We actively monitor CometBFT (formerly known as Tendermint) metrics from our nodes, including current block height, peer connections, mempool status, and standard host metrics like CPU usage, memory, and disk throughput. These metrics provide us with a comprehensive overview of each node's health and performance.

- Blackbox Monitoring:

In addition to internal metrics, we employ blackbox monitoring through our custom Open-source tool cosmos-validator-watcher. This tool checks our uptime by connecting simultaneously to internal and external RPCs and helps us ensure that no critical information is missed.

[

1600×1098 394 KB

](https://europe1.discourse-cdn.com/standard21/uploads/dymension/original/1X/ffec5c2112b43b97ae15b7208173ac4c6a321f12.jpeg)

The cosmos-validator-watcher extends beyond monitoring, offering insights into total stakes, reward commissions, and tracking our votes on current on-chain governance proposals.

Leveraging our GitOps workflow, the validator watcher enables us to automate the upgrade process through webhooks. This approach is more efficient than swapping out binaries (especially in an immutable container), a common practice with tools like Cosmovisor.

For those interested in a deeper dive into how our cosmos-validator-watcher operates, we've made the information available on our GitHub repository at GitHub - kilnfi/cosmos-validator-watcher: Real-time Cosmos-based chains monitoring.

## About Horcrux

Horcrux, a Multi-Party Computation (MPC) signing service for Tendermint nodes, enhances validator infrastructure security and availability by utilizing a cluster of signer nodes, ensuring fault tolerance, securing private keys through threshold Ed25519 signatures, and boosting performance. Explore the documentation to upgrade your validator infrastructure with Horcrux.

## About Kiln

Kiln is the leading enterprise-grade staking platform, enabling institutional customers to stake their digital assets programmatically and whitelabel staking functionality into their offerings. Kiln runs validators on all major PoS blockchains, with over $5b of stake under management. As an experienced Cosmos-based chains node operator, we offer staking services and real-time data for various chains, including DYM, ATOM, Osmosis, TIA, INJ, KAVA, and more, to fully meet our customers' requirements.